XML Examples for the Cisco Application Centric Infrastructure Security Device Package, Version 1.2(7)

Released: September 30, 2016

This document provides XML examples for the ASA features that are supported through the Application Policy Infrastructure Controller (APIC) northbound APIs. However, the document does not include a complete list of all the ASA feature options available for these services. To determine the options that the northbound APIs allow, you should use the *device_specification.xml* file that is provided with the ASA device package.

For information about how to use the APIC northbound APIs, see the *Cisco APIC Management Information Model Reference*.

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Available APIC Products

Starting with release 1.2(7), there are two versions of the Cisco ASA Device Package software for ACI, as described below:

- Cisco ASA Device Package software for ACI - This is the same as the original version that was available with version 1.2(6) and earlier. This version allows you to configure many important features of ASA from APIC, including but not limited to the following:
  - Interface
  - Routing
  - Access-list
  - NAT
  - TrustSec
  - Application inspection
  - NetFlow
  - High availability
- Cisco ASA Device Package Fabric Insertion software for ACI - This version contains the following subset of the features of the original version:
  - Interface
  - Dynamic routing
  - Static routing

Therefore, only the following XML examples apply to the Cisco ASA Device Package Fabric Insertion software for ACI:

Northbound API

The following is a sample XML for accessing the ASA. For a multi-context ASA, access information directly under vnsLDevVip is that of the admin context in the ASA; the one in the vnsCDev folder is that of the target user context. Again, admin context can be used as the target user context.

Only one context from a given multi-context ASA is allowed here.

```
<polUni>
    <fvTenant
        dn="uni/tn-tenant1"
        name="tenant1">
        <vnsLDevVip name="Firewall" devtype="PHYSICAL">
            <vnsRsMDevAtt tDn="uni/infra/mDev-CISCO-ASA-1.2"/>
            <!---Admin context access information ---/>
            <vnsCMgmt name="devMgmt" host="172.23.204.205"  port="443"/>
            <vnsCCred name="username" value="admin"/>
            <vnsCCredSecret name="password" value="somepassword"/>

            <vnsCDev name="ASA">
            <!---User context access information ---/>
                <vnsCMgmt name="devMgmt" host="172.23.204.123" port="443" />
                <vnsCCred name="username" value="admin" />
                <vnsCCredSecret name="password" value="otherpassword" />
            </vnsCDev>
        </vnsLDevVip>

    </fvTenant>
</polUni>
```

Interfaces

Interfaces are typically set up as part of the overall infrastructure on the APIC using a service graph. The graphs are associated with contracts, concrete devices, logical devices, and logical interfaces. The graphs also require the interface IP addresses to be in an appropriate range previously defined for the associated tenant. The graph setups show the various interface types. For an ASAv, interfaces are defined on the ASA itself using the physical interfaces; for the hardware ASAs, interfaces are defined using VLANs. The XML files to define the interfaces are the same, and the device package uses the "devtype" field (PHYSICAL or VIRTUAL) to determine the correct CLIs to send to the ASA for configuration. The "funcType" field (GoTo or GoThrough) determines whether the interfaces are for a transparent or routed firewall.

Transparent Bridge Group Virtual Interfaces

This XML example creates the following bridge group and adds bridge group members. The example is for a hardware ASA; VLANs are dynamically assigned.

ASA Configuration

```
interface GigabitEthernet0/0
 no nameif
 no security-level

interface GigabitEthernet0/0.987
 vlan 987
```

```
 nameif externalIf
 bridge-group 1
 security-level 50

interface GigabitEthernet0/1
 no nameif
 no security-level

interface GigabitEthernet0/1.986
 vlan 986
 nameif internalIf
 bridge-group 1
 security-level 100

interface BVI1
 ip address 10.10.10.2 255.255.255.0
```

XML Example

Define a graph and interfaces, then attach them to the tenant.

```xml
<polUni>
    <fvTenant name="tenant1">
        <vnsAbsGraph name = "WebGraph">
            <vnsAbsTermNodeCon name = "Input1">
                <vnsAbsTermConn name = "C1"/>
            </vnsAbsTermNodeCon>

            <!-- FW1 Provides FW functionality -->
            <vnsAbsNode name = "FW1" funcType="GoThrough">
                <vnsRsDefaultScopeToTerm
tDn="uni/tn-tenant1/AbsGraph-WebGraph/AbsTermNodeProv-Output1/outtmnl"/>

                <vnsAbsFuncConn name = "external" attNotify="yes">
                    <vnsRsMConnAtt tDn="uni/infra/mDev-CISCO-ASA-{dp_version}/mFunc-Firewall/mConn-external"
/>
                </vnsAbsFuncConn>

                <vnsAbsFuncConn name = "internal" attNotify="yes">
                    <vnsRsMConnAtt tDn="uni/infra/mDev-CISCO-ASA-{dp_version}/mFunc-Firewall/mConn-internal"
/>
                </vnsAbsFuncConn>

        <vnsAbsDevCfg>
            <vnsAbsFolder key="BridgeGroupIntf" name="1">
                <vnsAbsFolder key="IPv4Address" name="internalIfIP">
                    <vnsAbsParam key="ipv4_address" name="ipv4" value="10.10.10.2/255.255.255.0"/>
                    <vnsAbsParam key="ipv4_standby_address" name="ipv4s" value="10.10.10.3"/>
                </vnsAbsFolder>
            </vnsAbsFolder>

        <vnsAbsFolder key="Interface" name="internalIf">
         <vnsAbsFolder key="InterfaceConfig" name="internalIfCfg">
            <vnsAbsCfgRel key="bridge_group" name="intbridge" targetName="1"/>
            <vnsAbsParam key="security_level" name="internal_security_level" value="100"/>
         </vnsAbsFolder>
        </vnsAbsFolder>
        <vnsAbsFolder key="Interface" name="externalIf">
         <vnsAbsFolder key="InterfaceConfig" name="externalIfCfg">
            <vnsAbsCfgRel key="bridge_group" name="extbridge" targetName="1"/>
            <vnsAbsParam key="security_level" name="external_security_level" value="50"/>
         </vnsAbsFolder>
        </vnsAbsFolder>
```

```
        </vnsAbsDevCfg>

    <vnsAbsFuncCfg>
         <vnsAbsFolder key="ExIntfConfigRelFolder" name="ExtConfigA">
             <vnsAbsCfgRel key="ExIntfConfigRel" name="ExtConfigrel" targetName="externalIf"/>
             <vnsRsScopeToTerm tDn="uni/tn-tenant1/AbsGraph-WebGraph/AbsTermNodeProv-Output1/outtmnl"/>
             <vnsRsCfgToConn tDn="uni/tn-tenant1/AbsGraph-WebGraph/AbsNode-FW1/AbsFConn-external" />
         </vnsAbsFolder>

        <vnsAbsFolder key="InIntfConfigRelFolder" name="IntConfigA">
             <vnsAbsCfgRel key="InIntfConfigRel" name="InConfigrel" targetName="internalIf"/>
             <vnsRsScopeToTerm tDn="uni/tn-tenant1/AbsGraph-WebGraph/AbsTermNodeProv-Output1/outtmnl"/>
             <vnsRsCfgToConn tDn="uni/tn-tenant1/AbsGraph-WebGraph/AbsNode-FW1/AbsFConn-internal" />
        </vnsAbsFolder>
    </vnsAbsFuncCfg>

            <vnsRsNodeToMFunc tDn="uni/infra/mDev-CISCO-ASA-{dp_version}/mFunc-Firewall"/>
        </vnsAbsNode>

        <vnsAbsTermNodeProv name = "Output1">
            <vnsAbsTermConn name = "C6"/>
        </vnsAbsTermNodeProv>

        <vnsAbsConnection name = "CON1">
            <vnsRsAbsConnectionConns
tDn="uni/tn-tenant1/AbsGraph-WebGraph/AbsTermNodeCon-Input1/AbsTConn"/>
            <vnsRsAbsConnectionConns
tDn="uni/tn-tenant1/AbsGraph-WebGraph/AbsNode-FW1/AbsFConn-external"/>
        </vnsAbsConnection>

         <vnsAbsConnection name = "CON2" unicastRoute="no">
            <vnsRsAbsConnectionConns
tDn="uni/tn-tenant1/AbsGraph-WebGraph/AbsNode-FW1/AbsFConn-internal"/>
            <vnsRsAbsConnectionConns
tDn="uni/tn-tenant1/AbsGraph-WebGraph/AbsTermNodeProv-Output1/AbsTConn"/>
        </vnsAbsConnection>
    </vnsAbsGraph>

    </fvTenant>
</polUni>
```

Routed Firewall Interfaces

This XML example creates the following routed interfaces. The example is for a hardware ASA; VLANs are dynamically assigned.

ASA Configuration

```
interface GigabitEthernet0/0.655
 vlan 655
 mac-address 00aa.00bb.00cc standby 00ff.00ff.ffff
 nameif externalIf
 security-level 50
 ip address 20.20.20.20 255.255.255.0 standby 20.20.20.21

interface GigabitEthernet0/1.968
 vlan 968
 nameif internalIf
 security-level 100
 ip address 10.10.10.10 255.255.255.0 standby 10.10.10.11
```

XML Example

Define a graph, then attach it to the tenant.

```
polUni>
    <fvTenant name="tenant1">
    <vnsAbsGraph name = "WebGraph">

    <vnsAbsTermNodeCon name = "Input1">
        <vnsAbsTermConn name = "C1">
        </vnsAbsTermConn>
    </vnsAbsTermNodeCon>

    <!-- FW1 Provides FW functionality -->
    <vnsAbsNode name = "FW1">
        <vnsRsDefaultScopeToTerm tDn="uni/tn-tenant1/AbsGraph-WebGraph/AbsTermNodeProv-Output1/outtmnl"/>

        <vnsAbsFuncConn name = "external" attNotify="yes">
            <vnsRsMConnAtt tDn="uni/infra/mDev-CISCO-ASA-{dp_version}/mFunc-Firewall/mConn-external" />
        </vnsAbsFuncConn>

        <vnsAbsFuncConn name = "internal" attNotify="yes">
            <vnsRsMConnAtt tDn="uni/infra/mDev-CISCO-ASA-{dp_version}/mFunc-Firewall/mConn-internal" />
        </vnsAbsFuncConn>

        <vnsAbsDevCfg>
          <vnsAbsFolder key="Interface" name="internalIf">
           <vnsAbsFolder key="InterfaceConfig" name="internalIfCfg">
              <vnsAbsFolder key="IPv4Address" name="internalIfIP">
                  <vnsAbsParam key="ipv4_address" name="ipv4_internal" value="10.10.10.10/255.255.255.0"/>
                  <vnsAbsParam key="ipv4_standby_address" name="ipv4_internals" value="10.10.10.11"/>
              </vnsAbsFolder>
              <vnsAbsParam key="security_level" name="internal_security_level" value="100"/>
           </vnsAbsFolder>
          </vnsAbsFolder>
          <vnsAbsFolder key="Interface" name="externalIf">
           <vnsAbsFolder key="InterfaceConfig" name="externalIfCfg">
              <vnsAbsFolder key="IPv4Address" name="externalIfIP">
                  <vnsAbsParam key="ipv4_address" name="ipv4_external" value="20.20.20.20/255.255.255.0"/>
                  <vnsAbsParam key="ipv4_standby_address" name="ipv4_externals" value="20.20.20.21"/>
              </vnsAbsFolder>
              <vnsAbsParam key="security_level" name="external_security_level" value="50"/>
              <vnsAbsFolder key="mac_address" name="mac">
                  <vnsAbsParam key="active_mac" name="activemac" value="aa.bb.cc"/>
                  <vnsAbsParam key="standby_mac" name="stbymac" value="ff.ff.ffff"/>
              </vnsAbsFolder>
           </vnsAbsFolder>
          </vnsAbsFolder>
        </vnsAbsDevCfg>

        <vnsAbsFuncCfg>
            <vnsAbsFolder key="ExIntfConfigRelFolder" name="ExtConfig">
              <vnsAbsCfgRel key="ExIntfConfigRel" name="ExtConfigrel" targetName="externalIf"/>
              <vnsRsScopeToTerm tDn="uni/tn-tenant1/AbsGraph-WebGraph/AbsTermNodeProv-Output1/outtmnl"/>
              <vnsRsCfgToConn tDn="uni/tn-tenant1/AbsGraph-WebGraph/AbsNode-FW1/AbsFConn-external" />
            </vnsAbsFolder>

            <vnsAbsFolder key="InIntfConfigRelFolder" name="IntConfig">
              <vnsAbsCfgRel key="InIntfConfigRel" name="InConfigrel" targetName="internalIf"/>
              <vnsRsScopeToTerm tDn="uni/tn-tenant1/AbsGraph-WebGraph/AbsTermNodeProv-Output1/outtmnl"/>
              <vnsRsCfgToConn tDn="uni/tn-tenant1/AbsGraph-WebGraph/AbsNode-FW1/AbsFConn-internal" />
            </vnsAbsFolder>
```

```
            </vnsAbsFuncCfg>

            <vnsRsNodeToMFunc tDn="uni/infra/mDev-CISCO-ASA-{dp_version}/mFunc-Firewall"/>
        </vnsAbsNode>

        <vnsAbsTermNodeProv name = "Output1">
            <vnsAbsTermConn name = "C6">
            </vnsAbsTermConn>
        </vnsAbsTermNodeProv>

        <vnsAbsConnection name = "CON1">
            <vnsRsAbsConnectionConns tDn="uni/tn-tenant1/AbsGraph-WebGraph/AbsTermNodeCon-Input1/AbsTConn" />
            <vnsRsAbsConnectionConns tDn="uni/tn-tenant1/AbsGraph-WebGraph/AbsNode-FW1/AbsFConn-external" />
        </vnsAbsConnection>

        <vnsAbsConnection name = "CON2">
            <vnsRsAbsConnectionConns tDn="uni/tn-tenant1/AbsGraph-WebGraph/AbsNode-FW1/AbsFConn-internal" />
            <vnsRsAbsConnectionConns tDn="uni/tn-tenant1/AbsGraph-WebGraph/AbsTermNodeProv-Output1/AbsTConn" />
        </vnsAbsConnection>

    </vnsAbsGraph>

    <vzBrCP name="webCtrct">
        <vzSubj name="http">
                <vzRsSubjGraphAtt tnVnsAbsGraphName="WebGraph"/>
        </vzSubj>
    </vzBrCP>
  </fvTenant>
</polUni>
```

Port Channel Interfaces

This XML example creates the following port channel members and port channel interfaces (supported only on physical ASAs at this time).

ASA Configuration

```
interface GigabitEthernet0/0
 channel-group 2 mode active
 no nameif
 no security-level
 no ip address

interface GigabitEthernet0/1
 channel-group 1 mode active
 no nameif
 no security-level
 no ip address

interface Port-channel1.100
 vlan 100
 nameif externalIf
 security-level 50
 ip address 20.20.20.20 255.255.255.0 standby 20.20.20.21

interface Port-channel2.200
 vlan 200
 nameif internalIf
 ip address 10.10.10.10 255.255.255.0 standby 10.10.10.11
```

XML Example

Define the port channel members, graph, then attach them to the tenant.

```xml
<polUni>
    <fvTenant dn="uni/tn-tenant1" name="tenant1">
      <vnsLDevVip name="Firewall" funcType="GoTo" devtype="PHYSICAL">
        <vnsRsMDevAtt tDn="uni/infra/mDev-CISCO-ASA-{dp_version}"/>
         <vnsRsALDevToPhysDomP tDn="uni/phys-phys"/>
          <vnsCMgmt name="devMgmt" host="10.122.202.33" port="443" />
            <vnsCCred name="username" value="management-user"/>
            <vnsCCredSecret name="password"  value="cisco"/>
        <vnsDevFolder key="PortChannelMember" name="PC1a">
          <vnsDevParam key="port_channel_id" name="PC1a" value="1"/>
          <vnsDevParam key="interface" name="PC1a" value="Gig0/1"/>
        </vnsDevFolder>
        <vnsDevFolder key="PortChannelMember" name="PC2a">
          <vnsDevParam key="port_channel_id" name="PC2a" value="2"/>
          <vnsDevParam key="interface" name="PC2a" value="Gig0/0"/>
        </vnsDevFolder>
        </vnsLDevVip>
        <vnsLDevCtx ctrctNameOrLbl="webCtrct" graphNameOrLbl="WebGraph" nodeNameOrLbl="FW1">
            <vnsRsLDevCtxToLDev tDn="uni/tn-tenant1/lDevVip-Firewall"/>
            <vnsLIfCtx connNameOrLbl="internal">
                <vnsRsLIfCtxToBD tDn= "uni/tn-tenant1/BD-tenant1BD1"/>
                <vnsRsLIfCtxToLIf tDn="uni/tn-tenant1/lDevVip-Firewall/lIf-internalPC"/>
            </vnsLIfCtx>
            <vnsLIfCtx connNameOrLbl="external">
               <vnsRsLIfCtxToLIf tDn="uni/tn-tenant1/lDevVip-Firewall/lIf-externalPC"/>
                <vnsRsLIfCtxToBD tDn= "uni/tn-tenant1/BD-tenant1BD2"/>
            </vnsLIfCtx>
        </vnsLDevCtx>
    </fvTenant>
</polUni>


<polUni>
    <fvTenant name="tenant1">

    <vnsAbsGraph name = "WebGraph">

    <vnsAbsTermNodeCon name = "Input1">
        <vnsAbsTermConn name = "C1">
        </vnsAbsTermConn>
    </vnsAbsTermNodeCon>

    <!-- FW1 Provides FW functionality -->
    <vnsAbsNode name = "FW1">
        <vnsRsDefaultScopeToTerm tDn="uni/tn-tenant1/AbsGraph-WebGraph/AbsTermNodeProv-Output1/outtmnl"/>

        <vnsAbsFuncConn name = "external" attNotify="yes">
            <vnsRsMConnAtt tDn="uni/infra/mDev-CISCO-ASA-{dp_version}/mFunc-Firewall/mConn-external" />
        </vnsAbsFuncConn>

        <vnsAbsFuncConn name = "internal" attNotify="yes">
            <vnsRsMConnAtt tDn="uni/infra/mDev-CISCO-ASA-{dp_version}/mFunc-Firewall/mConn-internal" />
        </vnsAbsFuncConn>

        <vnsAbsDevCfg>
          <vnsAbsFolder key="Interface" name="internalIf">
           <vnsAbsFolder key="InterfaceConfig" name="internalIfCfg">
              <vnsAbsFolder key="IPv4Address" name="internalIfIP">
                 <vnsAbsParam key="ipv4_address" name="ipv4_internal" value="10.10.10.10/255.255.255.0"/>
```

```
                <vnsAbsParam key="ipv4_standby_address" name="ipv4_internals" value="10.10.10.11"/>
            </vnsAbsFolder>
            <vnsAbsParam key="security_level" name="internal_security_level" value="100"/>
          </vnsAbsFolder>

        </vnsAbsFolder>
        <vnsAbsFolder key="Interface" name="externalIf">
         <vnsAbsFolder key="InterfaceConfig" name="externalIfCfg">
            <vnsAbsFolder key="IPv4Address" name="externalIfIP">
                <vnsAbsParam key="ipv4_address" name="ipv4_external" value="20.20.20.20/255.255.255.0"/>
                <vnsAbsParam key="ipv4_standby_address" name="ipv4_externals" value="20.20.20.21"/>
            </vnsAbsFolder>
            <vnsAbsParam key="security_level" name="external_security_level" value="50"/>
         </vnsAbsFolder>
        </vnsAbsFolder>
      </vnsAbsDevCfg>

      <vnsAbsFuncCfg>
          <vnsAbsFolder key="ExIntfConfigRelFolder" name="ExtConfig">
            <vnsAbsCfgRel key="ExIntfConfigRel" name="ExtConfigrel" targetName="externalIf"/>
            <vnsRsScopeToTerm tDn="uni/tn-tenant1/AbsGraph-WebGraph/AbsTermNodeProv-Output1/outtmnl"/>
            <vnsRsCfgToConn tDn="uni/tn-tenant1/AbsGraph-WebGraph/AbsNode-FW1/AbsFConn-external" />
          </vnsAbsFolder>

          <vnsAbsFolder key="InIntfConfigRelFolder" name="IntConfig">
            <vnsAbsCfgRel key="InIntfConfigRel" name="InConfigrel" targetName="internalIf"/>
            <vnsRsScopeToTerm tDn="uni/tn-tenant1/AbsGraph-WebGraph/AbsTermNodeProv-Output1/outtmnl"/>
            <vnsRsCfgToConn tDn="uni/tn-tenant1/AbsGraph-WebGraph/AbsNode-FW1/AbsFConn-internal" />
          </vnsAbsFolder>

      </vnsAbsFuncCfg>

      <vnsRsNodeToMFunc tDn="uni/infra/mDev-CISCO-ASA-{dp_version}/mFunc-Firewall"/>
    </vnsAbsNode>

    <vnsAbsTermNodeProv name = "Output1">
        <vnsAbsTermConn name = "C6">
        </vnsAbsTermConn>
    </vnsAbsTermNodeProv>

    <vnsAbsConnection name = "CON1">
        <vnsRsAbsConnectionConns tDn="uni/tn-tenant1/AbsGraph-WebGraph/AbsTermNodeCon-Input1/AbsTConn" />
        <vnsRsAbsConnectionConns tDn="uni/tn-tenant1/AbsGraph-WebGraph/AbsNode-FW1/AbsFConn-external" />
    </vnsAbsConnection>

    <vnsAbsConnection name = "CON2">
        <vnsRsAbsConnectionConns tDn="uni/tn-tenant1/AbsGraph-WebGraph/AbsNode-FW1/AbsFConn-internal" />
        <vnsRsAbsConnectionConns tDn="uni/tn-tenant1/AbsGraph-WebGraph/AbsTermNodeProv-Output1/AbsTConn" />
    </vnsAbsConnection>

    </vnsAbsGraph>
  </fvTenant>
</polUni>

<polUni>
    <fvTenant name="tenant1">
    <vzBrCP name="webCtrct">
        <vzSubj name="http">
            <vzRsSubjGraphAtt tnVnsAbsGraphName="WebGraph"/>
        </vzSubj>
    </vzBrCP>
  </fvTenant>
</polUni>
```

Access Lists and Associated Access Groups

This XML example creates an access list and assigns it to an access group associated with an existing interface.

ASA Configuration

```
access-list ACL2 extended deny ip any any
access-list ACL2 extended permit icmp any any
access-list ACL1 extended permit tcp any any eq ssh
access-list ACL1 extended permit tcp any any eq https

access-group ACL2 in interface externalIf
access-group ACL1 out interface internalIf
```

XML Example

```
<polUni>
    <fvTenant name="tenant1">
        <vnsAbsGraph name = "WebGraph">
            <vnsAbsNode name = "FW1">
                <vnsAbsDevCfg>
                    <vnsAbsFolder key="AccessList" name="ACL1">
                        <vnsAbsFolder key="AccessControlEntry" name="ACE1">
                            <vnsAbsParam key="action" name="action1" value="permit"/>
                            <vnsAbsParam key="order" name="order1" value="1"/>
                            <vnsAbsFolder key="protocol" name="protocol1">
                                <vnsAbsParam key="name_number" name="pNN1" value="tcp"/>
                            </vnsAbsFolder>
                            <vnsAbsFolder key="destination_service" name="d1">
                                <vnsAbsParam key="operator" name="dop1" value="eq"/>
                                <vnsAbsParam key="low_port" name="dlp1" value="ssh"/>
                            </vnsAbsFolder>
                        </vnsAbsFolder>
                        <vnsAbsFolder key="AccessControlEntry" name="ACE2">
                            <vnsAbsParam key="action" name="action2" value="permit"/>
                            <vnsAbsParam key="order" name="order2" value="2"/>
                            <vnsAbsFolder key="protocol" name="protocol2">
                                <vnsAbsParam key="name_number" name="pNN2" value="tcp"/>
                            </vnsAbsFolder>
                            <vnsAbsFolder key="destination_service" name="d2">
                                <vnsAbsParam key="operator" name="dop2" value="eq"/>
                                <vnsAbsParam key="low_port" name="dlp2" value="https"/>
                            </vnsAbsFolder>
                        </vnsAbsFolder>
                    </vnsAbsFolder>
                    <vnsAbsFolder key="AccessList" name="ACL2">
                        <vnsAbsFolder key="AccessControlEntry" name="ACE1">
                            <vnsAbsParam key="action" name="action1" value="deny"/>
                            <vnsAbsParam key="order" name="order1" value="1"/>
                        </vnsAbsFolder>
                        <vnsAbsFolder key="AccessControlEntry" name="ACE2">
                            <vnsAbsParam key="action" name="action2" value="permit"/>
                            <vnsAbsParam key="order" name="order2" value="2"/>
                            <vnsAbsFolder key="protocol" name="protocol2">
                                <vnsAbsParam key="name_number" name="pNN2" value="icmp"/>
                            </vnsAbsFolder>
                        </vnsAbsFolder>
```

```
                            </vnsAbsFolder>
                            <vnsAbsFolder key="Interface" name="internalIf">
                             <vnsAbsFolder name="IntAccessGroup" key="AccessGroup">
                                  <vnsAbsCfgRel key="outbound_access_list_name" name="iACG"
targetName="ACL1"/>
                             </vnsAbsFolder>
                            </vnsAbsFolder>
                            <vnsAbsFolder key="Interface" name="externalIf">
                             <vnsAbsFolder name="ExtAccessGroup" key="AccessGroup">
                                  <vnsAbsCfgRel key="inbound_access_list_name" name="oACG"
targetName="ACL2"/>
                             </vnsAbsFolder>
                            </vnsAbsFolder>
                        </vnsAbsDevCfg>
                   </vnsAbsNode>
             </vnsAbsGraph>
     </fvTenant>
</polUni>
```

Access Lists Using Dynamically Created EPG Network Objects

This XML example creates an access list that dynamically updates the object group membership in the ACL, where the object group corresponds to an End Point Group (EPG).

Note You must create the necessary *AccessControlEntry* in APIC.

ASA Configuration

```
access-list EPG_ACL extended permit ip object-group __$EPG$_web object-group __$EPG$_app
access-group EPG_ACL in interface externalIf
```

XML Example

```
<polUni>
    <fvTenant name="tenant1">
        <vnsAbsGraph name = "WebGraph">
            <vnsAbsNode name = "FW1">
                <vnsAbsDevCfg>
                    <vnsAbsFolder key="AccessList" name="EPG_ACL">
                        <vnsAbsFolder key="AccessControlEntry" name="EPG_ACE">
                            <vnsAbsParam key="action" name="action1" value="permit"/>
                            <vnsAbsParam key="order" name="order1" value="1"/>
                            <vnsAbsFolder key="source_address" name="saddr1">
                                  <vnsAbsParam key="epg_name" name="webEPG"
value="tenantname-profilename-web"/>
                            </vnsAbsFolder>
                            <vnsAbsFolder key="destination_address" name="daddr1">
                                  <vnsAbsParam key="epg_name" name="appEPG"
value="tenantname-profilename-app"/>
                            </vnsAbsFolder>
                        </vnsAbsFolder>
                     </vnsAbsFolder>
                    <vnsAbsFolder key="Interface" name="externalIf">
                            <vnsAbsFolder name="access-group-EPG" key="AccessGroup">
```

```
                                                  <vnsAbsCfgRel name="name" key="inbound_access_list_name"
          targetName="EPG_ACL"/>
                                           </vnsAbsFolder>
                                    </vnsAbsFolder>
                              </vnsAbsDevCfg>
                        </vnsAbsNode>
                  </vnsAbsGraph>
            </fvTenant>
      </polUni>
```

IP Audit

This XML example sets up the IP audit attack configuration.

ASA Configuration

```
ip audit attack action drop
```

XML Example (Attack)

```
<polUni>
    <fvTenant name="tenant1">
        <vnsLDevVip name="Firewall">
                <vnsDevFolder key="IPAudit" name="A">
                    <vnsDevParam key="IPAuditAttack" name="IPattack" value="drop"/>
                </vnsDevFolder>
        </vnsLDevVip>
    </fvTenant>
</polUni>
```

XML Example (Info)

This XML example also sets up the IP audit attack configuration.

```
ip audit attack action reset
```

```
<polUni>
    <fvTenant name="tenant1">
        <vnsLDevVip name="Firewall">
                <vnsDevFolder key="IPAudit" name="A">
                    <vnsDevParam key="IPAuditInfo" name="IPinfo" value="reset"/>
                </vnsDevFolder>
        </vnsLDevVip>
    </fvTenant>
</polUni>
```

Logging

This XML example sets up the logging configuration.

ASA Configuration

```
logging enable
logging buffer-size 8192
logging buffered critical
logging trap alerts
```

XML Example

```xml
<polUni>
    <fvTenant name="tenant1">
        <vnsLDevVip name="Firewall">
                <vnsDevFolder key="LoggingConfig" name="Log">
                    <vnsDevParam key="enable_logging" name="enlog" value="enable"/>
                    <vnsDevParam key="buffered_level" name="bufflev" value="critical"/>
                <vnsDevParam key="buffer_size" name="buffsize" value="8192"/>
                <vnsDevParam key="trap_level" name="trap" value="1"/>
            </vnsDevFolder>
        </vnsLDevVip>
    </fvTenant>
</polUni>
```

Static Route

This XML example sets up the static route configuration that is associated with an existing interface.

ASA Configuration

```
route internalIf 10.100.0.0 255.255.0.0 10.6.55.1 1
```

XML Example

```xml
<polUni>
    <fvTenant name="tenant1">
        <vnsAbsGraph name = "WebGraph">
            <vnsAbsNode name = "FW1">
                <vnsAbsDevCfg>
                    <vnsAbsFolder key="Interface" name="internalIf">
                    <vnsAbsFolder key="StaticRoute" name="InsideRTE1">
                        <vnsAbsFolder key="route" name="RouteIN1">
                            <vnsAbsParam key="network" name="network1" value="10.100.0.0"/>
                            <vnsAbsParam key="netmask" name="netmask1" value="255.255.0.0"/>
                            <vnsAbsParam key="gateway" name="gateway1" value="10.6.55.1"/>
                            <vnsAbsParam key="metric" name="metric1" value="1"/>
                        </vnsAbsFolder>
                    </vnsAbsFolder>
                    </vnsAbsFolder>
```

```
                </vnsAbsDevCfg>
            </vnsAbsNode>
        </vnsAbsGraph>
    </fvTenant>
</polUni>
```

Basic Threat Detection

This XML example sets up a basic threat detection rate for an ACL drop.

ASA Configuration

```
threat-detection rate acl-drop rate-interval 600 average-rate 0 burst-rate 0
```

XML Example

```
<polUni>
    <fvTenant name="tenant1">
        <vnsLDevVip name="Firewall">
                <vnsDevFolder key="BasicThreatDetection" name="BasicTD">
                  <vnsDevParam key="basic_threat" name="Basic1" value="enable"/>
                  <vnsDevFolder key="BasicThreatDetectionRateAclDrop" name="BasicTDACL">
                      <vnsDevParam key="rate_interval" name="ri1" value="600"/>
                      <vnsDevParam key="average_rate" name="ar1" value="0"/>
                      <vnsDevParam key="burst_rate" name="br1" value="0"/>
                  </vnsDevFolder>
                </vnsDevFolder>
        </vnsLDevVip>
    </fvTenant>
</polUni>
```

Scanning Threat Detection

This XML example sets up the scanning threat detection rate.

ASA Configuration

```
threat-detection rate scanning-threat rate-interval 600 average-rate 100 burst-rate 40
threat-detection scanning-threat shun
```

XML Example

```
<polUni>
    <fvTenant name="tenant1">
        <vnsLDevVip name="Firewall">
                <vnsDevFolder key="ScanningThreatDetection" name="ScanTD1">
                    <vnsDevParam key="scanning_threat" name="Scan1" value="enable"/>
                    <vnsDevParam key="shun_status" name="Shun1" value="enable"/>
                    <vnsDevFolder key="ScanningThreatRate" name="ScanTDrate">
                        <vnsDevParam key="average_rate" name="ar1" value="100"/>
```

```
                      <vnsDevParam key="rate_interval" name="ri1" value="600"/>
                      <vnsDevParam key="burst_rate" name="br1" value="40"/>
                  </vnsDevFolder>
                  <vnsDevFolder key="ScanningThreatRate" name="ScanTDrate2">
                      <vnsDevParam key="average_rate" name="ar2" value="10"/>
                      <vnsDevParam key="rate_interval" name="ri2" value="660"/>
                      <vnsDevParam key="burst_rate" name="br2" value="20"/>
                  </vnsDevFolder>
              </vnsDevFolder>
          </vnsLDevVip>
      </fvTenant>
</polUni>
```

Advanced Threat Detection

This XML example sets up advanced threat detection statistics.

ASA Configuration

```
threat-detection statistics host
threat-detection statistics port number-of-rate 2
threat-detection statistics protocol number-of-rate 3
threat-detection statistics tcp-intercept rate-interval 50 burst-rate 200 average-rate 100
```

XML Example

```
<polUni>
    <fvTenant name="tenant1">
        <vnsLDevVip name="Firewall">
              <vnsDevFolder key="AdvancedThreatDetection" name="AdvScan" >
                  <vnsDevParam key="access_list" name="status5" value="enable"/>
                  <vnsDevFolder key="AdvancedThreatDetectionTcpIntercept" name="AdvScanTCPInt" >
                      <vnsDevParam key="status" name="AdvRateStatus" value="enable"/>
                      <vnsDevParam key="average_rate" name="AdvRate" value="100"/>
                      <vnsDevParam key="rate_interval" name="AdvRI" value="50"/>
                      <vnsDevParam key="burst_rate" name="AdvBR" value="200"/>
                  </vnsDevFolder>
                  <vnsDevFolder key="AdvancedThreatDetectionHost" name="AdvScanHost" >
                      <vnsDevParam key="status" name="HostStatus" value="enable"/>
                      <vnsDevParam key="number_of_rate" name="HostRate" value="1"/>
                  </vnsDevFolder>
                  <vnsDevFolder key="AdvancedThreatDetectionPort" name="AdvScanPort" >
                      <vnsDevParam key="status" name="PortStatus" value="enable"/>
                      <vnsDevParam key="number_of_rate" name="PortRate" value="2"/>
                  </vnsDevFolder>
                  <vnsDevFolder key="AdvancedThreatDetectionProtocol" name="AdvScanProtocol" >
                      <vnsDevParam key="status" name="ProtocolStatus" value="enable"/>
                      <vnsDevParam key="number_of_rate" name="ProtocolRate" value="3"/>
                  </vnsDevFolder>
              </vnsDevFolder>
        </vnsLDevVip>
    </fvTenant>
</polUni>
```

Protocol Timeouts

This XML example sets up the protocol timeout value for the connection timer.

ASA Configuration

```
timeout conn 2:00:59
```

XML Example

```
<polUni>
    <fvTenant name="tenant1">
        <vnsLDevVip name="Firewall">
                <vnsDevFolder key="Timeouts" name="TO">
                    <vnsDevParam key="Connection" name="conn1" value="2:0:59"/>
                </vnsDevFolder>
        </vnsLDevVip>
    </fvTenant>
</polUni>
```

Network Time Protocol

This XML example turns on the Network Time Protocol (NTP) feature that defines the server to use.

ASA Configuration

```
ntp server 192.168.100.100 prefer
```

XML Example

```
<polUni>
    <fvTenant name="tenant1">
        <vnsLDevVip name="Firewall">
            <vnsDevFolder key="NTP" name="NTP">
                <vnsDevFolder key="NTPServer" name="NTPServer">
                    <vnsDevParam key="server" name="server" value="192.168.100.100"/>
        <vnsDevParam key="prefer" name="prefer" value="enable"/>
                </vnsDevFolder>
            </vnsDevFolder>
        </vnsLDevVip>
    </fvTenant>
</polUni>
```

Smart Call-Home

This XML example turns on the Smart Call-Home feature with anonymous reporting.

ASA Configuration

```
call-home reporting anonymous
```

XML Example

```
<polUni>
    <fvTenant name="tenant1">
        <vnsLDevVip name="Firewall">
            <vnsDevFolder key="SmartCallHome" name="SmartCallHome">
                <vnsDevParam key="anonymous_reporting" name="anonymous_reporting" value="enable"/>
            </vnsDevFolder>
        </vnsLDevVip>
    </fvTenant>
</polUni>
```

Domain Name System

This XML example turns on the Domain Name System (DNS) feature, links it to the utility interface, and specifies which domain name and server IP to use.

ASA Configuration

> **Note** You must preconfigure the utility interface on the ASA using the **nameif management-utility** command.

```
dns domain-lookup management-utility
dns server-group DefaultDNS
 name-server 1.1.1.1
 domain-name testDomain
```

XML Example

```
<polUni>
    <fvTenant name="tenant1">
        <vnsLDevVip name="Firewall">
            <vnsDevFolder key="DNS" name="DNS">
                <vnsDevParam key="domain_name" name="domain_name" value="testDomain"/>
                <vnsDevParam key="name_server" name="name_server" value="1.1.1.1"/>
            </vnsDevFolder>
        </vnsLDevVip>
    </fvTenant>
</polUni>
```

Connection Limits

This XML example shows connection limits associated with interfaces (global connection limits are not supported), matches any traffic, and sets up the maximum number of connections that are allowed. Also included are connection limits on internal and external interfaces.

ASA Configuration

```
class-map connlimits_internalIf
 match any

policy-map internalIf
 class connlimits_internalIf
  set connection conn-max 654 embryonic-conn-max 456

service-policy internalIf interface internalIf
```

XML Example

```
<polUni>
    <fvTenant name="tenant1">
        <vnsAbsGraph name = "WebGraph">
            <vnsAbsNode name = "FW1">
                <vnsAbsDevCfg>
                  <vnsAbsFolder key="Interface" name="internalIf">
                      <vnsAbsFolder key="ServicePolicy" name="ConLim-Policy">
                          <vnsAbsParam key="ServicePolicyState" name="PolicyState" value="enable"/>
                          <vnsAbsFolder key="ConnectionLimits" name="ConnLim">
                              <vnsAbsFolder key="ConnectionSettings" name="ConnectionSettingsA">
                                  <vnsAbsParam key="conn_max" name="conn_max" value="654"/>
                                  <vnsAbsParam key="conn_max_embryonic" name="conn_max_embryonic"
value="456"/>
                              </vnsAbsFolder>
                          </vnsAbsFolder>
                      </vnsAbsFolder>
                  </vnsAbsFolder>
                </vnsAbsDevCfg>
            </vnsAbsNode>
        </vnsAbsGraph>
    </fvTenant>
</polUni>
```

Application Inspections

This XML example shows application inspections associated with interfaces (global application inspection is not supported), matches default inspection traffic, and enables HTTP inspection. Also included is application inspection on internal and external interfaces.

ASA Configuration

```
class-map inspection_internalIf
 match default-inspection-traffic
```

```
                    policy-map internalIf
                     class inspection_internalIf
                      inspect http

                    service-policy internalIf interface internalIf
```

XML Example

```
<polUni>
    <fvTenant name="tenant1">
        <vnsAbsGraph name = "WebGraph">
            <vnsAbsNode name = "FW1">
                <vnsAbsDevCfg>
                    <vnsAbsFolder key="Interface" name="internalIf">
                        <vnsAbsFolder key="ServicePolicy" name="Inspection-Policy">
                            <vnsAbsParam key="ServicePolicyState" name="PolicyState" value="enable"/>
                            <vnsAbsFolder key="ApplicationInspection" name="ApplicationInspection">
                                <vnsAbsFolder key="InspectionSettings" name="InspectionSettingsA">
                                    <vnsAbsParam key="http" name="http" value="enable"/>
                                </vnsAbsFolder>
                            </vnsAbsFolder>
                        </vnsAbsFolder>
                    </vnsAbsFolder>
                </vnsAbsDevCfg>
            </vnsAbsNode>
        </vnsAbsGraph>
    </fvTenant>
</polUni>
```

Global NetFlow

This XML example sets up the NetFlow feature. The example shows how to create a simple access list to which traffic is matched, creates a NetFlow object, and enables NetFlow globally for the NetFlow objects. Also included is NetFlow on internal and external interfaces.

ASA Configuration

```
                    class-map netflow_default
                     match any

                    flow-export destination management-utility 1.2.3.4 1024
                    flow-export template timeout-rate 120
                    flow-export delay flow-create 60
                    flow-export active refresh-interval 30

                    class netflow_default
                      flow-export event-type all destination 1.2.3.4
```

XML Example

```
<polUni>
    <fvTenant name="tenant1">
        <vnsLDevVip name="Firewall">
```

```
            <vnsDevFolder key="NetFlowObjects" name="ObjectA">
                <vnsDevFolder key="TemplateAndCollectors" name="TemplateA">
                    <vnsDevParam key="template_timeout_rate" name="timeout" value="120"/>
                    <vnsDevParam key="delay_flow_create" name="delay" value="60"/>
                    <vnsDevParam key="active_refresh_interval" name="refresh" value="30"/>
                    <vnsDevFolder key="NetFlowCollectors" name="CollectorA">
                        <vnsDevParam key="status" name="status" value="enable"/>
                        <vnsDevParam key="host" name="host" value="1.2.3.4"/>
                        <vnsDevParam key="port" name="port" value="1024"/>
                    </vnsDevFolder>
                </vnsDevFolder>
            </vnsDevFolder>
            <vnsDevFolder key="GlobalServicePolicy" name="GlobalPolicyA">
                <vnsDevParam key="ServicePolicyState" name="PolicyState" value="enable"/>
                <vnsDevFolder key="NetFlow" name="NetFlowPolicyA">
                    <vnsDevFolder key="NetFlowSettings" name="SettingA">
                        <vnsDevFolder key="ExportAllEvent" name="ExportAll">
                            <vnsDevParam key="status" name="status" value="enable"/>
                            <vnsDevParam key="event_destination" name="dest" value="1.2.3.4"/>
                        </vnsDevFolder>
                    </vnsDevFolder>
                </vnsDevFolder>
            </vnsDevFolder>
        </vnsLDevVip>
    </fvTenant>
</polUni>
```

Network Address Translation

This XML example sets up the Network Address Translation (NAT) feature on the external interface, based on the previously created network objects, *ilinux1* and *olinux1*.

ASA Configuration

```
nat (externalIf,internalIf) source static ilinux1 olinux1
```

XML Example

```
<polUni>
    <fvTenant name="tenant1">
        <vnsAbsGraph name = "WebGraph">
            <vnsAbsNode name = "FW1">
                <vnsAbsDevCfg>
                    <vnsAbsFolder key="NATList" name="ListA">
                        <vnsAbsFolder key="NATRule" name="RuleA">
                            <vnsAbsParam key="order" name="order" value="3"/>
                            <vnsAbsFolder key="source_translation" name="source_trans">
                                <vnsAbsFolder key="mapped_object" name="mapped_object">
                                    <vnsAbsCfgRel key="object_name" name="map_name" targetName="olinux1"/>
                                 </vnsAbsFolder>
                                <vnsAbsFolder key="real_object" name="real_object">
                                    <vnsAbsCfgRel key="object_name" name="real_name" targetName="ilinux1"/>
                                 </vnsAbsFolder>
                                <vnsAbsParam key="nat_type" name="nat_type" value="static"/>
                            </vnsAbsFolder>
                        </vnsAbsFolder>
```

```
                    </vnsAbsFolder>
                </vnsAbsDevCfg>
                <vnsAbsFuncCfg>
                    <vnsAbsFolder key="NATPolicy" name="PolicyA">
                        <vnsAbsCfgRel key="nat_list_name" name="nat_listA" targetName="ListA"/>
                    </vnsAbsFolder>
                </vnsAbsFuncCfg>
            </vnsAbsNode>
        </vnsAbsGraph>
    </fvTenant>
</polUni>
```

Intrusion Prevention System

This XML example sets up the Intrusion Prevention System (IPS) feature. The example shows how to match traffic to a previously created access list, *ACL1,* and enables IPS as inline and fail-open. Also included is IPS on internal and global interfaces.

ASA Configuration

```
class-map ips_internalIf
 match access-list ACL1

policy-map internalIf
 class ips_internalIf
  ips inline fail-open

service-policy internalIf interface internalIf
```

XML Example

```
<polUni>
    <fvTenant name="tenant1">
        <vnsAbsGraph name = "WebGraph">
            <vnsAbsNode name = "FW1">
                <vnsAbsDevCfg>
                  <vnsAbsFolder key="Interface" name="internalIf">
                      <vnsAbsFolder key="ServicePolicy" name="IPS-Policy">
                          <vnsAbsParam key="ServicePolicyState" name="PolicyState" value="enable"/>
                          <vnsAbsFolder key="IPS" name="IPS">
                             <vnsAbsCfgRel key="TrafficSelection" name="TrafficSelect" targetName="ACL1"/>
                             <vnsAbsFolder key="IPSSettings" name="IPSSettingsA">
                                  <vnsAbsParam key="operate_mode" name="operate_mode" value="inline"/>
                                  <vnsAbsParam key="fail_mode" name="fail_mode" value="fail-open"/>
                              </vnsAbsFolder>
                          </vnsAbsFolder>
                      </vnsAbsFolder>
                  </vnsAbsFolder>
                </vnsAbsDevCfg>
            </vnsAbsNode>
        </vnsAbsGraph>
    </fvTenant>
</polUni>
```

SourceFire

This XML example shows a basic SourceFire configuration in fail-open and monitor-only mode.

ASA Configuration

```
access-list ACL1 extended permit ip any any
class-map sfr_internalIf
 match access-list ACL1
policy-map internalIf
 class sfr_internalIf
  sfr fail-open monitor-only
```

XML Example

```
<polUni>
    <fvTenant name="tenant1">
        <vnsAbsGraph name = "WebGraph">
            <vnsAbsNode name = "FW1">
                <vnsAbsDevCfg>
                    <vnsAbsFolder key="AccessList" name="ACL1">
                        <vnsAbsFolder key="AccessControlEntry" name="ACE1">
                            <vnsAbsParam key="action" name="action1" value="permit"/>
                            <vnsAbsParam key="order" name="order1" value="1"/>
                        </vnsAbsFolder>
                    </vnsAbsFolder>
                    <vnsAbsFolder key="Interface" name="internalIf">
                      <vnsAbsFolder key="ServicePolicy" name="SFR-Policy">
                        <vnsAbsParam key="ServicePolicyState" name="PolicyState"
value="enable"/>
                        <vnsAbsFolder key="SFR" name="SFR">
                          <vnsAbsCfgRel key="TrafficSelection" name="TrafficSelect"
targetName="ACL1"/>
                          <vnsAbsFolder key="SFRSettings" name="SFRSettings">
                            <vnsAbsParam key="monitor_only" name="operate_mode"
value="enable"/>
                            <vnsAbsParam key="fail_mode" name="fail_mode"
value="fail-open"/>
                          </vnsAbsFolder>
                        </vnsAbsFolder>
                      </vnsAbsFolder>
                    </vnsAbsFolder>
                </vnsAbsDevCfg>
            </vnsAbsNode>
        </vnsAbsGraph>
    </fvTenant>
</polUni>
```

Network Objects

This XML example sets up a network object with a host IP address and description.

ASA Configuration

```
object network ilinux1
 host 192.168.1.48
 description User1 laptop
```

XML Example

```
<polUni>
    <fvTenant name="tenant1">
        <vnsAbsGraph name = "WebGraph">
            <vnsAbsNode name = "FW1">
                <vnsAbsDevCfg>
                    <vnsAbsFolder key="NetworkObject" name="ilinux1">
                        <vnsAbsParam key="host_ip_address" name="host_ip_address" value="192.168.1.48"/>
                        <vnsAbsParam key="description" name="description" value="User1 laptop"/>
                    </vnsAbsFolder>
                </vnsAbsDevCfg>
            </vnsAbsNode>
        </vnsAbsGraph>
    </fvTenant>
</polUni>
```

Network Object Groups

This XML example sets up a network object group with a group name and group objects.

ASA Configuration

```
object-group network Cisco-Network-Object-GroupA
 description Cisco inside network
 network-object host 192.168.1.51
```

XML Example

```
<polUni>
    <fvTenant name="tenant1">
        <vnsAbsGraph name = "WebGraph">
            <vnsAbsNode name = "FW1">
                <vnsAbsDevCfg>
                    <vnsAbsFolder key="NetworkObjectGroup" name="Cisco-Network-Object-GroupA">
                        <vnsAbsParam key="description" name="description" value="Cisco inside network"/>
                        <vnsAbsParam key="host_ip_address" name="host_ip_address" value="192.168.1.51"/>
                    </vnsAbsFolder>
                </vnsAbsDevCfg>
            </vnsAbsNode>
        </vnsAbsGraph>
```

```
        </fvTenant>
</polUni>
```

High Availability (Failover)

This XML example enables failover and specifies the failover interface and IP addresses.

ASA Configuration

```
failover
failover lan unit primary
failover lan interface fover GigabitEthernet0/0
failover interface ip fover 192.168.17.1 255.255.255.0 standby 192.168.17.2
```

XML Example

```
<polUni>
    <fvTenant name="tenant1">
        <vnsLDevVip name="Firewall">
         <vnsLIf name="failover_lan">
           <vnsRsMetaIf
tDn="uni/infra/mDev-CISCO-ASA-{dp_version}/mIfLbl-failover_lan"/>
           <vnsRsCIfAtt
tDn="uni/tn-tenant1/lDevVip-Firewall/cDev-ASAP/cIf-[Gig0/0]"/>
         </vnsLIf>
          <vnsCDev name="ASAP">
                <vnsDevFolder key="FailoverConfig" name="failover_config">
                    <vnsDevParam key="failover" name="failover" value="enable"/>
                    <vnsDevParam key="lan_unit" name="lan_unit" value="primary"/>
                    <vnsDevFolder key="failover_lan_interface" name="failover_lan">
                        <vnsDevParam key="interface_name" name="interface_name" value="fover"/>
                    </vnsDevFolder>
                    <vnsDevFolder key="failover_ip" name="failover_ip">
                        <vnsDevParam key="interface_name"  name="interface_name" value="fover"/>
                        <vnsDevParam key="active_ip"  name="primary_ip" value="192.168.17.1"/>
                        <vnsDevParam key="netmask"  name="netmask" value="255.255.255.0"/>
                        <vnsDevParam key="standby_ip"  name="secondary_ip" value="192.168.17.2"/>
                    </vnsDevFolder>
                </vnsDevFolder>
            </vnsCDev>
        </vnsLDevVip>
    </fvTenant>
</polUni>
```

TCP Service Reset

This XML example sends a Reset Reply for Denied Inbound/Outbound TCP Packets.

ASA Configuration

```
service resetinbound | resetoutbount interface interface_name
```

XML Example

```
<fvTenant name="tenant1">
        <vnsAbsGraph name = "WebGraph">
            <vnsAbsNode name = "FW1">
                <vnsAbsDevCfg>
                    <vnsAbsFolder key="Interface" name="externalIf">
                    <vnsAbsFolder name="TCPOpt" key="TCPOptions">"
                    <vnsAbsParam key="inbound_reset" name="reset" value="disable"/>
                    </vnsAbsFolder>
                    </vnsAbsFolder>
                </vnsAbsDevCfg>
            </vnsAbsNode>
        </vnsAbsGraph>
    </fvTenant>
</polUni>
```

Support for Cisco TrustSec

Creating a Security Object Group

```
<polUni>
    <fvTenant name="tenant1">
        <vnsAbsGraph name = "WebGraph">
            <vnsAbsNode name = "FW1">
                <vnsAbsDevCfg>
                    <vnsAbsFolder key="SecurityObjectGroup" name="coke_sec_obj">
                        <vnsAbsParam key="security_group_name" name="sg1" value="mktg"/>
                    </vnsAbsFolder>
                </vnsAbsDevCfg>
            </vnsAbsNode>
        </vnsAbsGraph>
    </fvTenant>
</polUni>
```

Creating a Security Group ACL

```
<polUni>
<fvTenant name="tenant1\">
<vnsAbsGraph name = "WebGraph">
<vnsAbsNode name = "FW1">
    <vnsAbsDevCfg>
        <vnsAbsFolder key="AccessList" name="FROM-OUTSIDE">
```

```
                <vnsAbsFolder key="AccessControlEntry" name="ACE1">
                    <vnsAbsParam key="action" name="action1" value="permit"/>
                    <vnsAbsParam key="order" name="order1" value="1"/>
                    <vnsAbsFolder key="protocol" name="prot1">
                        <vnsAbsParam key="name_number" name="NN" value="icmp"/>
                    </vnsAbsFolder>
                    <vnsAbsFolder key="source_security_group" name="security_group_name">
                        <vnsAbsParam key="security_group_name" name="security_group_name" value="coke-sec-obj"/>
                    </vnsAbsFolder>
                </vnsAbsFolder>
            </vnsAbsFolder>
        </vnsAbsDevCfg>
</vnsAbsNode>
</vnsAbsGraph>
</fvTenant>
</polUni>


---------


<polUni>
<fvTenant name="tenant1\">
<vnsAbsGraph name = "WebGraph">
<vnsAbsNode name = "FW1">
    <vnsAbsDevCfg>
        <vnsAbsFolder key="AccessList" name="TEST-ACL">
            <vnsAbsFolder key="AccessControlEntry" name="ACE1">
                <vnsAbsParam key="action" name="action1" value="permit"/>
                <vnsAbsParam key="order" name="order10" value="10"/>
                <vnsAbsFolder key="protocol" name="protocol">
                    <vnsAbsParam key="name_number" name="name_number" value="tcp"/>
                </vnsAbsFolder>
                <vnsAbsFolder key="source_security_group" name="source_security_group">
                    <vnsAbsCfgRel key="security_object_group" name="security_object_group"
targetName="paris"/>
                </vnsAbsFolder>
                <vnsAbsFolder key="destination_service" name="destination_service">
                    <vnsAbsParam key="high_port" name="high_port" value="2000"/>
                    <vnsAbsParam key="low_port" name="low_port" value="800"/>
                    <vnsAbsParam key="operator" name="operator" value="eq"/>
                </vnsAbsFolder>
            </vnsAbsFolder>
        </vnsAbsFolder>
    </vnsAbsDevCfg>
</vnsAbsNode>
</vnsAbsGraph>
</fvTenant>
</polUni>
```

Configuring AAA-Server ISE for TrustSec

```
test1_trustSecxml='''\
<polUni>
    <fvTenant name="tenant1">
        <vnsLDevVip name="Firewall">
            <vnsDevFolder key="TrustSec" name="TrustSec">
                <vnsDevFolder key="ISEServerGroup" name="ise">
                    <vnsDevFolder key="AAAServer" name="ise">
                        <vnsDevParam key="host" name="host" value="192.168.102.241"/>
                        <vnsDevParam key="key" name="key" value="cisco123"/>
                    </vnsDevFolder>
                </vnsDevFolder>
            </vnsDevFolder>
```

```
        </vnsLDevVip>
    </fvTenant>
</polUni>
'''
```

Manually Assigning a Security Group Tag (SGT) to an IP Host Mapping Manually

```
test2_trustSecxml='''\
<polUni>
    <fvTenant name="tenant1">
        <vnsLDevVip name="Firewall">
            <vnsDevFolder key="TrustSec" name="TrustSec">
                <vnsDevFolder key="TrustSecSGTMap" name="SGTMap">
                    <vnsDevParam key="ip_address" name="ip_address" value="30.30.30.100"/>
                    <vnsDevParam key="security_group_tag" name="tag" value="100"/>
                </vnsDevFolder>
                <vnsDevFolder key="TrustSecSGTMap" name="SGTMap2">
                    <vnsDevParam key="ip_address" name="ip_address" value="2001:3030:30::112"/>
                    <vnsDevParam key="security_group_tag" name="tag" value="65519"/>
                </vnsDevFolder>
            </vnsDevFolder>
        </vnsLDevVip>
    </fvTenant>
</polUni>
'''
```

Configuring a TrustSec SXP Configuration to Get SGT From an AAA-Server

```
test3_trustSecxml='''\
<polUni>
    <fvTenant name="tenant1">
        <vnsLDevVip name="Firewall">
            <vnsDevFolder key="TrustSec" name="TrustSec">
                <vnsDevFolder key="SXP" name="SXP">
                    <vnsDevParam key="default_password" name="default_password" value="cisco123"/>
                    <vnsDevParam key="retry_period" name="retry_period" value="60"/>
                    <vnsDevParam key="enable" name="enable" value="true"/>
                    <vnsDevParam key="reconciliation_period" name="reconciliation_period" value="60"/>
                </vnsDevFolder>
            </vnsDevFolder>
        </vnsLDevVip>
    </fvTenant>
</polUni>
'''
```

Configuring a SXP Listener and Speaker

```
test4_trustSecxml='''\
<polUni>
    <fvTenant name="tenant1">
        <vnsLDevVip name="Firewall">
            <vnsDevFolder key="TrustSec" name="TrustSec">
                <vnsDevFolder key="SXP" name="SXP">
```

```
                <vnsDevFolder key="peer" name="peer">
                    <vnsDevParam key="password" name="password" value="default"/>
                    <vnsDevParam key="ip_address" name="ip_address" value="192.168.102.240"/>
                    <vnsDevParam key="mode" name="mode" value="local"/>
                    <vnsDevParam key="role" name="mode" value="listener"/>
                </vnsDevFolder>
                <vnsDevFolder key="peer" name="peer2">
                    <vnsDevParam key="password" name="password" value="default"/>
                    <vnsDevParam key="ip_address" name="ip_address" value="2001:3030:30::112"/>
                    <vnsDevParam key="mode" name="mode" value="local"/>
                    <vnsDevParam key="role" name="mode" value="listener"/>
                </vnsDevFolder>
            </vnsDevFolder>
          </vnsDevFolder>
        </vnsLDevVip>
    </fvTenant>
</polUni>
'''
```

New remark Keyword for the access-list Command

ASA Configuration

```
access-list ACL2 remark Remarkable1
access-list ACL2 extended permit tcp any any
access-list ACL2 remark Remarkable2
access-list ACL2 extended permit udp any any
access-list ACL2 remark Remarkable3
access-list ACL2 extended permit icmp any any
```

XML Example

```
<polUni>
<fvTenant name="tenant1\">
<vnsAbsGraph name = "WebGraph">
<vnsAbsNode name = "FW1">
    <vnsAbsDevCfg>
    <vnsAbsFolder key="AccessList" name="ACL2">
        <vnsAbsFolder key="AccessControlEntry" name="ACE2">
            <vnsAbsParam key="action" name="action1" value="permit"/>
            <vnsAbsParam key="order" name="order1" value="1"/>
            <vnsAbsParam key="remark" name="remark1" value="Remarkable1"/>
            <vnsAbsFolder key="protocol" name="protocol1">
            <vnsAbsParam key="name_number" name="pNN1" value="tcp"/>
            </vnsAbsFolder>
        </vnsAbsFolder>
        <vnsAbsFolder key="AccessControlEntry" name="ACE3">
            <vnsAbsParam key="action" name="action1" value="permit"/>
            <vnsAbsParam key="order" name="order3" value="3"/>
            <vnsAbsParam key="remark" name="remark2" value="Remarkable2"/>
            <vnsAbsFolder key="protocol" name="protocol3">
            <vnsAbsParam key="name_number" name="pNN3" value="udp"/>
            </vnsAbsFolder>
        </vnsAbsFolder>
        <vnsAbsFolder key="AccessControlEntry" name="ACE4">
            <vnsAbsParam key="action" name="action1" value="permit"/>
            <vnsAbsParam key="order" name="order4" value="4"/>
```

```
            <vnsAbsParam key="remark" name="remark3" value="Remarkable3"/>
            <vnsAbsFolder key="protocol" name="protocol4">
            <vnsAbsParam key="name_number" name="pNN4" value="icmp"/>
            </vnsAbsFolder>
        </vnsAbsFolder>
    </vnsAbsFolder>
    </vnsAbsDevCfg>
</vnsAbsNode>
</vnsAbsGraph>
</fvTenant>
</polUni>
```

Global Application-Inspections

ASA Configuration

```
policy-map global_policy
class inspection_default
  inspect rsh
  inspect dns preset_dns_map
  inspect rtsp
  inspect h323 h225
  inspect skinny
  inspect sip
  inspect ip-options
  inspect xdmcp
  inspect sunrpc
  inspect sqlnet
  inspect tftp
  inspect h323 ras
  inspect esmtp
  inspect netbios
 inspect ftp
```

XML Example

```
<polUni>
    <fvTenant name="tenant1">
        <vnsLDevVip name="Firewall">
            <vnsDevFolder key="GlobalServicePolicy" name="GlobalServicePolicy">
                <vnsDevParam key="ServicePolicyState" name="ServicePolicyState" value="enable"/>
                <vnsDevFolder key="ApplicationInspection" name="ApplicationInspection">
                    <vnsDevFolder key="InspectionSettings" name="InspectionSettings">
                        <vnsDevParam key="tftp" name="tftp" value="enable"/>
                        <vnsDevParam key="rtsp" name="rtsp" value="enable"/>
                        <vnsDevParam key="h323_h225" name="h323_h225" value="enable"/>
                        <vnsDevParam key="skinny" name="skinny" value="enable"/>
                        <vnsDevParam key="sip" name="sip" value="enable"/>
                        <vnsDevParam key="esmtp" name="esmtp" value="enable"/>
                        <vnsDevParam key="ftp" name="ftp" value="enable"/>
                        <vnsDevParam key="h323_ras" name="h323_ras" value="enable"/>
                        <vnsDevParam key="sunrpc" name="sunrpc" value="enable"/>
                        <vnsDevParam key="ip_options" name="ip_options" value="enable"/>
                        <vnsDevParam key="xdmcp" name="xdmcp" value="enable"/>
                        <vnsDevParam key="sqlnet" name="sqlnet" value="enable"/>
                        <vnsDevParam key="dns_preset" name="dns_preset" value="enable"/>
                        <vnsDevParam key="netbios" name="netbios" value="enable"/>
```

```
                        <vnsDevParam key="rsh" name="rsh" value="enable"/>
                    </vnsDevFolder>
                </vnsDevFolder>
            </vnsDevFolder>
        </vnsLDevVip>
    </fvTenant>
</polUni>
```

New same-security-traffic Command

ASA Configuration

```
Same-security-traffic permit inter-interface
Same-security-traffic permit intra-interface
```

XML Example

```
<polUni>
    <fvTenant name="tenant1">
        <vnsLDevVip name="Firewall">
            <vnsDevFolder key="SameSecurityTraffic" name="SameSecurityTraffic">
                <vnsDevParam key="inter_interface" name="inter_interface" value="permit"/>
                <vnsDevParam key="intra_interface" name="intra_interface" value="permit"/>
            </vnsDevFolder>
        </vnsLDevVip>
    </fvTenant>
</polUni>
```

New time-range Command

ASA Configuration

```
time-range T1-time-range
 absolute start 08:09 07 August 2016 end 12:20 23 September 2018
 periodic Tuesday Thursday 8:09 to 20:00
 periodic Wednesday 5:07 to Tuesday 17:00

access-list example-list extended permit ip any any time-range T1-time-range
```

XML Example

```
<polUni>
    <fvTenant name="tenant1\">
        <vnsAbsGraph name = "WebGraph">
            <vnsAbsNode name = "FW1">
                <vnsAbsDevCfg>
                    <vnsAbsFolder key="TimeRange" name="T1-time-range">
                        <vnsAbsFolder key="AbsoluteTimeDate" name="AbsoluteTimeDate">
                            <vnsAbsFolder key="End" name="End">
```

```
                        <vnsAbsParam key="year" name="year" value="2016" />
                        <vnsAbsParam key="day" name="day" value="23" />
                        <vnsAbsParam key="month" name="month" value="09" />
                        <vnsAbsParam key="time" name="time" value="12:20" />
                    </vnsAbsFolder>
                    <vnsAbsFolder key="Start" name="Start">
                        <vnsAbsParam key="year" name="year2" value="2014" />
                        <vnsAbsParam key="day" name="day" value="07" />
                        <vnsAbsParam key="month" name="month" value="8" />
                        <vnsAbsParam key="time" name="time" value="8:9" />
                    </vnsAbsFolder>
                </vnsAbsFolder>
                <vnsAbsFolder key="WeeklyPeriod" name="WeeklyPeriod">
                    <vnsAbsParam key="start_day" name="start_day" value="Wednesday" />
                    <vnsAbsParam key="end_day" name="end_day" value="Tuesday" />
                    <vnsAbsParam key="start_time" name="start_time" value="5:7" />
                    <vnsAbsParam key="end_time" name="end_time" value="17:00" />
                </vnsAbsFolder>
                <vnsAbsFolder key="DailyPeriod" name="DailyPeriod">
                    <vnsAbsParam key="day" name="day" value="Tuesday Thursday" />
                    <vnsAbsParam key="start_time" name="start_time" value="8:9" />
                    <vnsAbsParam key="end_time" name="end_time" value="20:00" />
                </vnsAbsFolder>
            </vnsAbsFolder>
        </vnsAbsDevCfg>
    </vnsAbsNode>
  </vnsAbsGraph>
 </fvTenant>
</polUni>
```