XML Examples for the Cisco Application Centric Infrastructure Security Device Package

Released: August 6, 2014
Revised: November 10, 2014

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*.

- Interfaces, page 2
- Access Lists and Associated Access Groups, page 8
- IP Audit, page 10
- Logging, page 10
- Static Route, page 11
- Threat Detection, page 12
- Protocol Timeouts, page 13
- Network Time Protocol, page 14
- Smart Call-Home, page 14
- Domain Name System, page 15
- Connection Limits, page 15
- Application Inspections, page 16
- Global NetFlow, page 17
- Network Address Translation, page 18
- Intrusion Prevention System, page 19
- Network Objects, page 19

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

- Network Object Groups, page 20
- High Availability (Failover), page 21

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.

```
<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">
                    <vnsRsMConnAtt tDn="uni/infra/mDev-CISCO-ASA-1.0.1.43/mFunc-Firewall/mConn-external" />
                </vnsAbsFuncConn>

                <vnsAbsFuncConn name = "internal">
                    <vnsRsMConnAtt tDn="uni/infra/mDev-CISCO-ASA-1.0.1.43/mFunc-Firewall/mConn-internal" />
                </vnsAbsFuncConn>

       <vnsAbsDevCfg>
          <vnsAbsFolder key="BridgeGroupIntf" name="1">
                <vnsAbsParam key="ipv4_address" name="ipv4" value="10.10.10.2/255.255.255.0"/>
           </vnsAbsFolder>
          <vnsAbsFolder key="Interface" name="internalIf">
           <vnsAbsFolder key="InterfaceConfig" name="internalIfCfg">
               <vnsAbsCfgRel key="bridge_group" name="extbridge" 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-1.0.1.43/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
 no nameif
 no security-level
 no ip address

interface GigabitEthernet0/0.655
 vlan 655
 nameif externalIf
 security-level 50
 ip address 10.10.10.10 255.255.255.0

interface GigabitEthernet0/1
 no nameif
 no security-level
 no ip address

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

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">
            <vnsRsMConnAtt tDn="uni/infra/mDev-CISCO-ASA-1.0.1.43/mFunc-Firewall/mConn-external" />
        </vnsAbsFuncConn>
        <vnsAbsFuncConn name = "internal">
            <vnsRsMConnAtt tDn="uni/infra/mDev-CISCO-ASA-1.0.1.43/mFunc-Firewall/mConn-internal" />
        </vnsAbsFuncConn>

        <vnsAbsDevCfg>
           <vnsAbsFolder key="Interface" name="internalIf">
            <vnsAbsFolder key="InterfaceConfig" name="internalIfCfg">
                <vnsAbsParam key="ipv4_address" name="ipv4_internal" value="10.10.10.10/255.255.255.0"/>
                <vnsAbsParam key="security_level" name="internal_security_level" value="100"/>
            </vnsAbsFolder>
           </vnsAbsFolder>
           <vnsAbsFolder key="Interface" name="externalIf">
           <vnsAbsFolder key="InterfaceConfig" name="externalIfCfg">
                <vnsAbsParam key="ipv4_address" name="ipv4_external" value="10.10.10.10/255.255.255.0"/>
                <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-1.0.1.43/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>
```

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 10.10.10.10 255.255.255.0

interface Port-channel2.200
 vlan 200
 nameif internalIf
 security-level 100
 ip address 10.10.10.10 255.255.255.0
```

XML Example

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

```
<polUni>
    <fvTenant
    dn="uni/tn-tenant1"
    name="tenant1">
        <vnsLDevVip name="Firewall">
            <vnsCDev name="ASA">
               <vnsCIf name="port-channel1">
                    <vnsRsCIfPathAtt tDn="topology/pod-1/paths-101/pathep-[eth1/20]"/>
               </vnsCIf>
               <vnsCIf name="port-channel2">
                    <vnsRsCIfPathAtt tDn="topology/pod-1/paths-101/pathep-[eth1/21]"/>
               </vnsCIf>

                <vnsCMgmt name="devMgmt" host="10.122.202.34" 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>

            </vnsCDev>
        </vnsLDevVip>

    </fvTenant>
</polUni>



<polUni>
    <fvTenant name="tenant1">

        <!-- Graph info -->
    <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">
            <vnsRsMConnAtt tDn="uni/infra/mDev-CISCO-ASA-1.0.1.43/mFunc-Firewall/mConn-external" />
        </vnsAbsFuncConn>

        <vnsAbsFuncConn name = "internal">
            <vnsRsMConnAtt tDn="uni/infra/mDev-CISCO-ASA-1.0.1.43/mFunc-Firewall/mConn-internal" />
        </vnsAbsFuncConn>

        <vnsAbsDevCfg>
           <vnsAbsFolder key="Interface" name="internalIf">
            <vnsAbsFolder key="InterfaceConfig" name="internalIfCfg">
                <vnsAbsParam key="ipv4_address" name="ipv4_internal" value="10.10.10.10/255.255.255.0"/>
                <vnsAbsParam key="security_level" name="internal_security_level" value="100"/>
            </vnsAbsFolder>

           </vnsAbsFolder>
           <vnsAbsFolder key="Interface" name="externalIf">
            <vnsAbsFolder key="InterfaceConfig" name="externalIfCfg">
                <vnsAbsParam key="ipv4_address" name="ipv4_external" value="10.10.10.10/255.255.255.0"/>
                <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-1.0.1.43/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>
```

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

```
<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

```
<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>
```

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 (Basic Threat Detection)

```
<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_status" name="rs1" value="enable"/>
                        <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>
```

XML Example (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
```

```
<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="status" name="r1" value="enable"/>
                        <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>
        </vnsLDevVip>
    </fvTenant>
</polUni>
```

XML Example (Advanced Threat Detection)

This XML example sets up advanced threat detection statistics.

ASA Configuration

```
threat-detection statistics protocol number-of-rate 3
threat-detection statistics access-list
threat-detection statistics tcp-intercept rate-interval 50 burst-rate 200 average-rate 100
```

```
<polUni>
    <fvTenant name="tenant1">
        <vnsLDevVip name="Firewall">
                <vnsDevFolder key="AdvancedThreatDetection" name="AdvScan" >
                    <vnsDevParam key="statistics" name="statistics" value="enable"/>
                    <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="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>
```

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="Firewall²>
<vnsLIf name="failover_lan">
                <vnsRsMetaIf
tDn="uni/infra/mDev-CISCO-ASA-1.0.1/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>
```

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.