Cisco Application Centric Infrastructure Security Device Package, Version 1.2(3) の XML の例

リリース日:2015 年 9 月 1 日

このドキュメントでは、Application Policy Infrastructure Controller（APIC）のノースバウンド API を通じてサポートされる ASA 機能の XML の例を示します。ただし、このマニュアルには、これらのサービスで利用可能なすべての ASA 機能オプションの完全なリストは含まれていません。ノースバウンド API で使用可能なオプションを特定するには、ASA デバイス パッケージに同梱されている *device_specification.xml* ファイルを使用してください。

APIC ノースバウンドの API の使用方法については、『*Cisco APIC Management Information Model Reference (Cisco APIC 管理情報モデルのリファレンス)*』を参照してください。

ノースバウンド API

次に、ASA にアクセスするための XML の例を示します。マルチコンテキスト ASA の場合、vnsLDevVip 直下にあるアクセス情報は、ASA の管理コンテキストのアクセス情報であり、vnsCDev フォルダ内の情報は対象ユーザ コンテキストのアクセス情報です。この場合も、管理コンテキストを対象ユーザ コンテキストとして使用できます。

ここでは、所定のマルチコンテキスト ASA からの 1 つのコンテキストだけを使用できます。

```
<polUni>
    <fvTenant
        dn="uni/tn-tenant1"
        name="tenant1">
        <vnsLDevVip name="Firewall" devtype="PHYSICAL">
            <vnsRsMDevAtt tDn="uni/infra/mDev-CISCO-ASA-1.2"/>
            <!---管理コンテキスト アクセス情報 ---/>
            <vnsCMgmt name="devMgmt" host="172.23.204.205"  port="443"/>
            <vnsCCred name="username" value="admin"/>
            <vnsCCredSecret name="password" value="somepassword"/>

            <vnsCDev name="ASA">
            <!---ユーザ コンテキスト アクセス情報 ---/>
                <vnsCMgmt name="devMgmt" host="172.23.204.123" port="443" />
                <vnsCCred name="username" value="admin" />
                <vnsCCredSecret name="password" value="otherpassword" />
            </vnsCDev>
        </vnsLDevVip>

    </fvTenant>
</polUni>
```

インターフェイス

通常、インターフェイスは、サービス グラフを使用する APIC インフラストラクチャ全体の一部としてセットアップされます。これらのグラフは契約、具体的なデバイス、論理デバイス、および論理インターフェイスに関連付けられます。グラフには、関連付けられたテナントについてこれまでに定義されている適切な範囲内のインターフェイス IP アドレスも必要です。グラフのセットアップでは、さまざまなインターフェイス タイプが表示されます。ASAv については、物理インターフェイスを使用してインターフェイスが ASA 自体で定義されます。ハードウェア ASA については、VLAN を使用してインターフェイスが定義されます。インターフェイスを定義する XML ファイルは同じであるため、デバイス パッケージは「devtype」フィールド（PHYSICAL または VIRTUAL）を使用して ASA に送信する適切な CLI を特定し、設定を行います。「funcType」フィールド（GoTo または GoThrough）によって、インターフェイスがトランスペアレント ファイアウォール用かルーテッド ファイアウォール用かが特定されます。

トランスペアレント ブリッジ グループの仮想インターフェイス

この XML の例では、次のブリッジ グループを作成してブリッジ グループのメンバを追加します。次に、ハードウェア ASA の例を示します。VLAN は動的に割り当てられます。

ASA の設定

```
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 の例

グラフとインターフェイスを定義し、それらをテナントに付与します。

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

            <!-- FW1 によって FW 機能が指定されます -->
            <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>
```

ルーテッド ファイアウォール インターフェイス

この XML の例では、次のルーテッド インターフェイスを作成します。次に、ハードウェア ASA の例を示します。VLAN は動的に割り当てられます。

ASA の設定

```
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 の例

グラフを定義し、そのグラフをテナントに付与します。

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

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

    <!-- FW1 によって FW 機能が指定されます -->
    <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>
```

ポート チャネル インターフェイス

この MXL の例では、次のポート チャネル メンバとポート チャネル インターフェイスを作成します(この時点で物理 ASA上でサポートされている場合のみ)。

ASA の設定

```
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 の例

ポート チャネル メンバ、グラフを定義し、それらをテナントに付与します。

```
<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 によって FW 機能が指定されます -->
    <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>
```

アクセス リストと関連アクセス グループ

この XML の例では、アクセス リストを作成し、そのリストを既存のインターフェイスと関連付けられたアクセス グループに割り当てます。

ASA の設定

```
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 の例

```
<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>
```

動的に作成された EPG ネットワーク オブジェクトを使用するアクセス リスト

この XML の例では、オブジェクト グループがエンド ポイント グループに対応している場合に、ACL 内のオブジェクト グループ メンバーシップを動的に更新するアクセス リストを作成します。

メモ 必要な *AccessControlEntry* を APIC に作成する必要があります。

ASA の設定

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

XML の例

```
<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 監査

この XML の例では、IP 監査攻撃の設定をセットアップします。

ASA の設定

```
ip audit attack action drop
```

XML の例（攻撃）

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

XML の例（情報）

この XML の例でも、IP 監査攻撃の設定をセットアップします。

```
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>
```

ロギング

この XML の例では、ロギングの設定をセットアップします。

ASA の設定

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

XML の例

```
<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>
```

スタティック ルート

この XML の例では、既存のインターフェイスに関連付けられたスタティック ルートの設定をセットアップします。

ASA の設定

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

XML の例

```
<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>
```

基本的な脅威検出

この XML の例では、ACL ドロップ用の基本的な脅威検出レートの設定をセットアップします。

ASA の設定

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

XML の例

```
<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>
```

スキャン脅威検出

この XML の例では、スキャン脅威検出レートをセットアップします。

ASA の設定

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

XML の例

```
<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>
```

高度な脅威検出

この XML の例では、高度な脅威検出の統計情報をセットアップします。

ASA の設定

```
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 の例

```
<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>
```

プロトコルのタイムアウト

この XML の例では、接続タイマーのプロトコル タイムアウト値をセットアップします。

ASA の設定

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

XML の例

```
<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

この XML の例では、使用するサーバを定義する Network Time Protocol（NTP）機能をオンにします。

ASA の設定

```
ntp server 192.168.100.100 prefer
```

XML の例

```
<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

この XML の例では、Smart Call-Home 機能と匿名レポートをオンにします。

ASA の設定

```
call-home reporting anonymous
```

XML の例

```
<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>
```

ドメイン ネーム システム

この XML の例では、ドメイン ネーム システム（DNS）機能をオンにし、それをユーティリティ インターフェイスにリンクし、使用するドメイン名とサーバ IP を指定します。

ASA の設定

メモ **nameif management-utility** コマンドを使用して、ユーティリティ インターフェイスを ASA 上に事前に設定しておく必要があります。

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

XML の例

```
<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>
```

接続制限

この XML の例では、インターフェイスに関連付けられた接続制限を示し（グローバル接続制限はサポートされていません）、トラフィックを照合し、許可する最大接続数をセットアップします。内部インターフェイスと外部インターフェイスの接続制限も含まれています。

ASA の設定

```
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 の例

```
<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>
```

アプリケーション インスペクション

この XML の例では、インターフェイスに関連付けられたアプリケーション インスペクションを示し（グローバル アプリケーション インスペクションはサポートされていません）、デフォルトのインスペクション トラフィックを照合し、HTTP インスペクションを有効にします。内部インターフェイスと外部インターフェイスのアプリケーション インスペクションも含まれています。

ASA の設定

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

policy-map internalIf
 class inspection_internalIf
  inspect http

service-policy internalIf interface internalIf
```

XML の例

```
<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>
```

グローバル NetFlow

この XML の例では、NetFlow 機能をセットアップします。この例では、トラフィックを照合する簡単なアクセス リストの作成方法を示し、NetFlow オブジェクトを作成し、その NetFlow オブジェクトに対してグローバルに NetFlow を有効にします。また、内部インターフェイスと外部インターフェイスの NetFlow も含まれます。

ASA の設定

```
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 の例

```
<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>
```

ネットワーク アドレス変換

この XML の例では、以前に作成したネットワーク オブジェクトの *ilinux1* と *olinux1* に基づいて、ネットワーク アドレス変換（NAT）機能を外部インターフェイス上にセットアップします。

ASA の設定

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

XML の例

```
<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>
```

侵入防御システム

この XML の例では、侵入防御システム（IPS）機能をセットアップします。この例では、以前に作成したアクセスリストの *ACL1* とトラフィックとの照合方法を示し、IPS をインラインおよびフェールオープンとして有効にします。内部インターフェイスとグローバル インターフェイスの IPS も含まれています。

ASA の設定

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

policy-map internalIf
 class ips_internalIf
  ips inline fail-open

service-policy internalIf interface internalIf
```

XML の例

```
<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

この XML の例では、フェールオープンおよびモニタ専用モードでの基本的な SourceFire 設定を示します。

ASA の設定

```
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 の例

```
<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>
```

ネットワーク オブジェクト

この XML の例では、ホスト IP アドレスおよび説明とともにネットワーク オブジェクトをセットアップします。

ASA の設定

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

XML の例

```
<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>
```

ネットワーク オブジェクト グループ

この XML の例では、グループ名およびグループ オブジェクトとともにネットワーク オブジェクト グループをセットアップします。

ASA の設定

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

XML の例

```
<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>
```

高可用性（フェールオーバー）

この XML の例では、フェールオーバーを有効にし、フェールオーバー インターフェイスと IP アドレスを指定します。

ASA の設定

```
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 の例

```
<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 サービスのリセット

この XML の例では、拒否された着信/発信 TCP パケットに対するリセット応答を送信します。

ASA の設定

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

XML の例

```
<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>
```