Policy APIs: Getting Started Guide

Software Version 1.0

vmware

Table of Contents

1. Overview

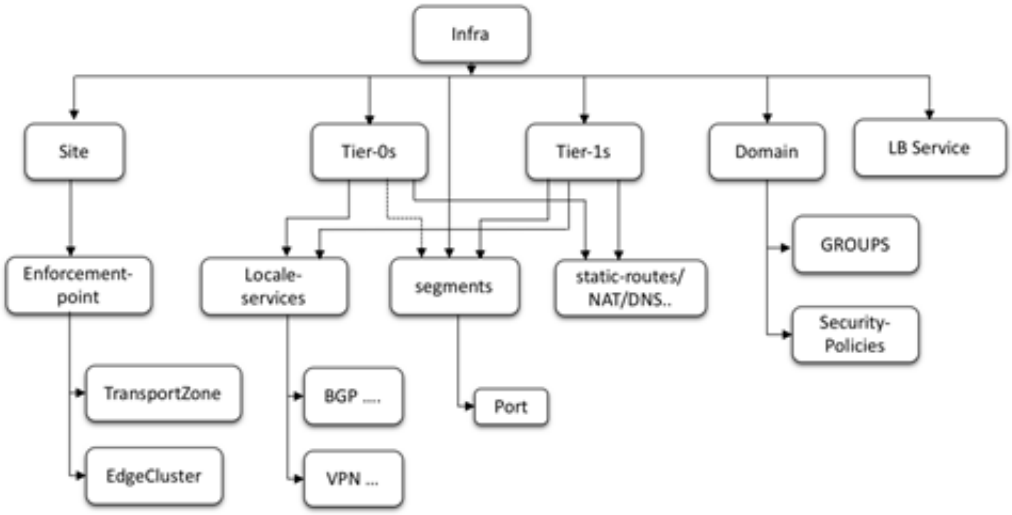
Policy APIs provide a simplified data model and allows the consumption of different services using an intent-based approach. It uses a declarative API model and can be used to create the entire intent in one go without caring about ordering or having to make multiple API calls. The intent is expressed using the parent/child relationship between the objects. The data model guarantees that a parent object is created before its child object, making it order independent. The model also allows for a user defined object ID to be specified whilst creating an object. Each object can be referenced by providing the full path of the object hierarchy.

The Policy API is also sometimes referred to as the hierarchical API and should not be confused with a Security Policy (in a DFW context).

The APIs operate on Policy objects and are provided under the hierarchical API endpoint:

```
/policy/api/v1/infra/
```

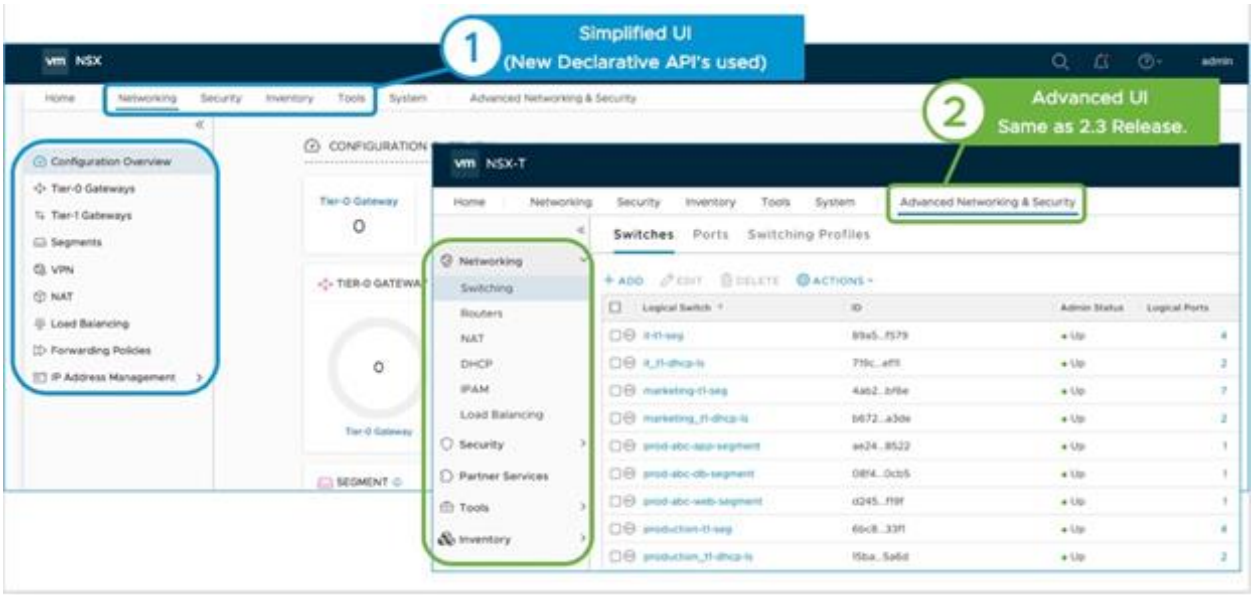
This API endpoint allows you to configure multiple objects (Segments, Gateways, Security Policies etc.) using a single API call. A very high-level overview of the hierarchy is shown below:



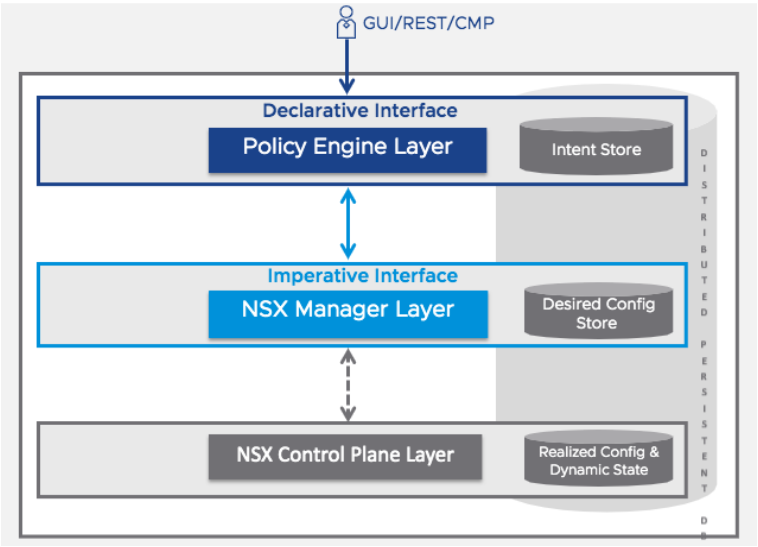
2. Consumption Model

From NSX-T 2.4 release, a user has two options to interact with NSX Manager:

1. Simplified UI (Declarative/Policy APIs)
    a. New interface introduced from NSX-T 2.4 release which uses the Declarative Policy API data model
2. Going forward, Simplified UI/Policy API should be used to manage NSX-T. Advanced UI (Imperative/MP APIs)
    a. All objects created till NSX-T 2.3 will be available in this data model.



There is a very clear separation that is defined between objects created with Policy APIs vs objects created using MP APIs.



NSX-T Declarative Policy Management Plane Architecture

Objects created using Policy API will be visible as Management Plane (MP) objects after realization. A call to a Policy API defines an intended state and realization happens in MP. Note that objects created using MP API are not visible to Policy API and cannot be seen in the Simplified UI.

Today, Policy objects refer to the logical constructions like:

- Tier-0/Tier-1 Gateway
- Segment
- Distributed Firewall
- Load Balancer
- DHCP etc

Policy objects do NOT include the unified appliance node (or cluster of nodes), Transport Nodes (Host and Edge), Edge Clusters and Transport Zones.

2.1. Naming changes

Starting with NSX-T 2.4 release, some of the logical objects are referred with new names. The below table summarizes the changes:

Existing Construct	New Construct	Definition
Logical switch	Segment	A network entity equivalent to a Logical Switch.
T1 Logical Router	Tier-1 Gateway	This is an entity equivalent to T1 router and allows the topology to scale out. Multiple Tier-1 Gateway talk with a Tier-0 Gateway.
T0 Logical Router	Tier-0 Gateway	This is an entity equivalent to T0 router and allows the Tier-1 to talk with outside world.
N/A	Domain	A logical construct represents the environment. Default domain represents entire NSX clusters. This is more relevant to Security policies.
NSGroup, IP Sets, MAC Sets	Group	Grouping construct to group the different objects statically and dynamically. This could be inventory entities like VMs, IPs, Mac etc.
Firewall section	Security-Policy	A structure to encompass various security policies, Section. Each security policy would have set of firewall rules.
Firewall rule	Rule	A structure to encompass various security related policies.
Edge Firewall	Gateway Firewall	Tier-0/Tier-1 Edge Firewall capability for north-south traffic.

3. Declarative API Data Model

The Policy APIs are declarative in nature and follow a parent-child hierarchical tree structure. Each node has a property named “resource_type” that specifies the node type (Gateway, Segments etc). It also contains a property named “children” that contains all the child objects of that node. The complete list of child objects can be found in the respective object schema. When describing the configuration in JSON, an additional wrapper layer is also used. Let’s look at the snippet below:

```
{
    "resource_type": "infra",
    "marked_for_delete": "false"
    "children": [
        {
            "resource_type": "ChildService",
            "marked_for_delete": "false",
            "Service": {
                ….
                ….
                "resource_type": "Service",
                "display_name": "My_Service",
                "id": "My_Service"
            }
        },
        {
            "resource_type": "ChildDomain",
            "marked_for_delete": "false",
            "Domain": {
                ….
                ….
                "resource_type": "Domain",
                "display_name": "My_Domain",
                "id": "My_Domain"
            }
        }
    ]
}
```

In the above snippet, the child objects of the Infra node is not the actual Service and Domain nodes. Instead, they are nested inside an intermediary node of the type ChildService and ChildDomain. These wrappers have a property named "resource_type" (Service and Domain in the example) containing the actual object configuration. Few things to note:

- The "resource_type" property is case sensitive
- If the "id" is not specified, the "display_name" property is used as the object ID
- The "id" is the user defined object ID and can be used in the full path while referring to an object

  Example:

```
{
    ….
    ….
    "resource_type": "Rule",
    "id": "my-app-rule-01",
    "display_name": "Web to DB Rule",
    "source_groups": [
        "/infra/domains/default/groups/WEB"
    ],
    "source_groups": [
        "/infra/domains/default/groups/DB"
    ]
    ….
    ….
}
```

4. Concurrency control

In order to prevent one client from overwriting another client's updates, NSX-T employs a technique called optimistic concurrency control.

All REST payloads contain a property named "*_revision*". This is an integer that is incremented each time an existing resource is updated. Clients must provide this property in PUT requests and it must match the current *_revision* or the update will be rejected. This guards against the following situation:

- Client 1 reads resource A.
- Client 2 reads resource A.
- Client 1 replaces the *display_name* property of resource A and does a PUT to replace the resource.
- Client 2 replaces a different property of resource A and attempts to perform a PUT operation.
- Without optimistic concurrency control, Client 2's update would overwrite Client 1's update to the *display_name* property. Instead, Client 2 receives a 409 Conflict error. To recover, Client 2 must fetch the resource again, apply the change, and perform a PUT.

However, Policy APIs also accept PATCH REST calls, which by default does not require that the *_revision* property be provided. A client can, however, request that the *_request* property be checked when it is performing a PATCH in the /infra path. To do this, the client should pass the query parameter *enforce_revision_check*. E.g.

```
PATCH /policy/api/v1/infra?enforce_revision_check=true
```

5. Operations

5.1. Creation (PATCH / PUT)

Policy APIs support the use of PATCH to interact with the objects. When a PATCH call is used, a new object is created if one doesn't exist and if the object already exists, then it updates the object. Note that _revision number checks are disabled by default on a PATCH call. Objects are updated as per the JSON body supplied regardless of its current configuration. Enforcing of the revision can be done by supplying the query parameter:

```
PATCH /policy/api/v1/infra?enforce_revision_check=true
```

When a PUT call is used, a new object is created if one doesn't exist as expected. However, if an object already exists, then it enforces the revision check before updating an existing object. It assumes a GET is performed to retrieve the existing config and the _revision number is sent via the PUT. If the _revision number matches current _revision, object is updated else an error is returned.

5.2. Deletion (DELETE / PATCH)

A typical deletion of the configuration can be done by performing the DELETE call against each object in that configuration. This results in multiple calls plus the object relationship has to be kept in mind. Alternatively, the hierarchical API can be leveraged to delete the complete or partial configuration using the PATCH call. In such a case, the "marked_for_delete" flag is set to "true" for the object(s) to be deleted. The snippet below deletes the Service object only:

```
PATCH /policy/api/v1/infra

JSON Body:

{

    "resource_type": "infra",

    "marked_for_delete": "false"
```

```
    "children": [
        {
            "resource_type": "ChildService",
            "marked_for_delete": "true",
            "Service": {
                ….
                ….
                "resource_type": "Service",
                "display_name": "My_Service",
                "id": "My_Service"
            }
        },
        {
            "resource_type": "ChildDomain",
            "marked_for_delete": "false",
            "Domain": {
                ….
                ….
                "resource_type": "Domain",
                "display_name": "My_Domain",
                "id": "My_Domain"
            }
        }
    ]
}
```

5.3. Retrieving Config with filters (GET)

The complete object config can be retrieved by performing the GET API with specific filter type:

```
GET /policy/api/v1/infra?filter=Type-
```

Note that the "filter" type can be passed only to the base URL. This specific API can take some time to return based on the configuration size in the system. Retrieving information about specific objects can be done by passing different filter types:

To Retrieve all Tier-1s:

```
GET /policy/api/v1/infra?filter=Type-Tier1
```

The above retrieves only the Tier-1 objects. If the Segments under the Tier1s are needed, then:

```
GET /policy/api/v1/infra?filter=Type-Tier1|Segment
```

The above retrieves both Flexible and Fixed Segments.

To retrieve basic Tier-0 configuration:

```
GET /policy/api/v1/infra?filter=Type-
Tier0|LocaleServices|Bgp|Tier0Interface|PolicyNat|PrefixList
```

To retrieve basic Tier-1 configuration:

```
GET /policy/api/v1/infra?filter=Type-Tier1|LocaleServices|PolicyNat
```

Filter all rule objects:

```
GET /policy/api/v1/infra?filter=Type-Domain|SecurityPolicy|Rule
```

Retrieve the whole intent tree except Services, LB, DHCP and MAC

```
GET /policy/api/v1/infra?filter=Type-(?i)^(?!(?:Service|LB|Dhcp|Mac)).*$
```

5.4. Importing API Spec

You can download the OpenAPI specifications for the NSX-T Policy APIs at the following URIs:

```
GET /api/v1/spec/openapi/nsx_policy_api.yaml
```

```
GET /api/v1/spec/openapi/nsx_policy_api.json
```

API Spec for managing objects in NSX-T for VMware Cloud on AWS can be downloaded at:

```
GET /api/v1/spec/openapi/nsx_vmc_policy_api.yml
GET /api/v1/spec/openapi/nsx_vmc_policy_api.json
```

6. Realization

When an API to create an object in Policy is called (through PATCH or PUT), a successful 200 return code ensures that the system knows about the intent. Actual realization happens in the system and can take longer. This could be due to the number of objects being created using the hierarchical API. In such a case, alarms are generated, and the following APIs can be used to check them:

```
GET /policy/api/v1/infra/realized-state/alarms
```

Every configured item will have an "intent path" or just "path". Examples are:

```
/infra/domains/default/groups/WEB
/infra/ip-pools/TEP-pool
```

The following 2 APIs can be used to validate if the intent has been realized on the configured endpoint:

- Realization status: Used to retrieve the overall realization status of the specified intent path

  ```
  GET /policy/api/v1/infra/realized-state/status?intent_path=<intent_path>
  ```

- Realized entities: Used to retrieve the realized objects on the endpoint for the specified intent

  ```
  GET /policy/api/v1/infra/realized-state/realized-
  entities?intent_path=<intent_path>
  ```

Note: The system reads the fabric configuration at 5 min intervals and watches for changes every 1 second for realization.

The status of the Policy service can be retrieved by

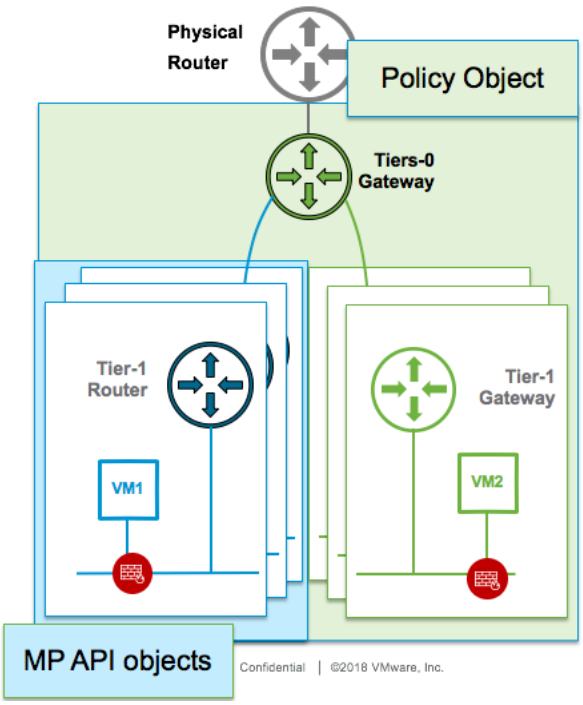
```
GET /api/v1/node/services/policy/status
```

7. Migrating from existing MP objects

There are a few things to consider if you are working with existing MP objects and want to transition to Policy objects. The two main cases when this can occur:

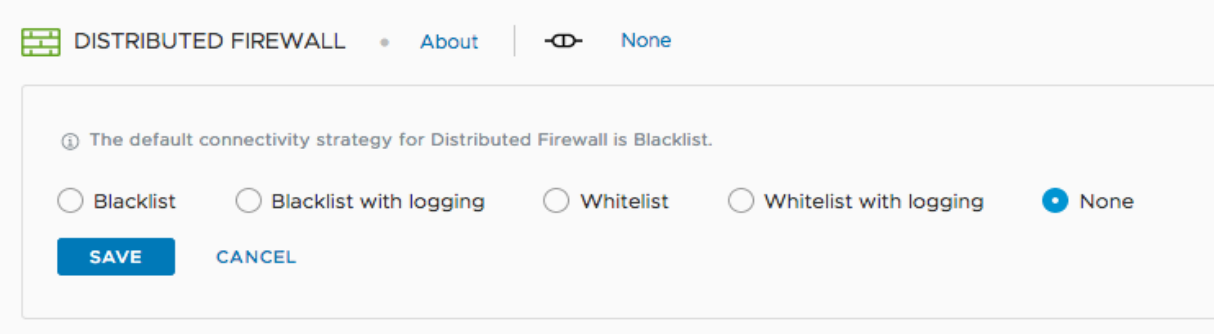
1. Upgrade: After an Upgrade, existing objects will appear under the Advanced UI and will continue to work. Interaction with these objects will be through MP APIs
2. Working with Content Management Systems in the case of OpenStack, Containers, vRA, CAS: These systems use MP APIs even when working with NSX-T 2.4. Transition into using Policy APIs are scheduled but till then all objects created will be shown under the Advanced UI

In both these cases, existing objects will continue to work and new Policy objects can be created. However, in order for them to co-exist, the following topology is recommended.



Creating the Tier-0 Gateway as a Policy Object and then connecting existing MP Tier-1 router or new Tier-1 Gateways to it. This will ensure existing topologies created using MP Objects can work with new Policy Objects. Overtime, the MP Objects can age out and only Policy objects can be used.

From a security standpoint, it is important to enforce Security from either MP or Policy. If all existing security policies are done through the Advanced UI, then to continue using it, make sure the Policy default is set to None and the use of Apply-To is strictly adhered to.



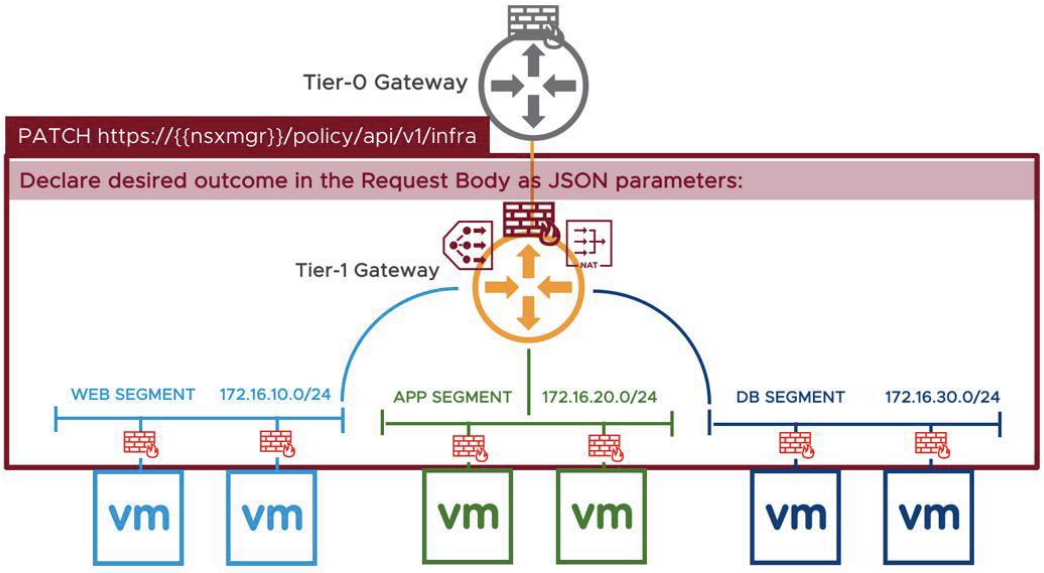
Do not combine Policy rules and MP rules to avoid stepping over each other and make sure there is only one Default rule specified. Better to start building with Policy rules today to minimize impact of moving from MP to Policy later

8. Examples

To get you started with the declarative API, 2 customer examples are provided here.

8.1. Example 1: 3-Tier App

In the first example, a 3-tier app is being deployed using the declarative API



Note that the Tier-0 Gateway is a Policy Object and is created outside the scope of the example. The declarative API creates the following in a single call:

Networking:

1. Create Tier-1 Router and attach to Tier-0
2. Create 3 Segments and attach to Tier-1 Gateway

3. Add NAT Stateful Service

Security:

1. Create Groups App Tier
2. Create Intra-app DFW policy
3. Create Gateway Firewall for Tier-1 GW

Load Balancer:

1. Create LB configuration - Profile, VIP, Pool, Certificates

```
curl -X PATCH \
  https://nsx-appliance.mylab.net/policy/api/v1/infra/ \
  -H 'authorization: Basic YWRtaW46Vk13YXJlIW1ncjE5Oak=' \
  -H 'cache-control: no-cache' \
  -H 'content-type: application/json' \
  -d '{
  "resource_type": "Infra",
  "children": [
    {
      "resource_type": "ChildTier1",
      "marked_for_delete": false,
      "Tier1": {
        "resource_type": "Tier1",
        "id": "DEV-tier-1-gw",
        "description": "DEV-tier-1-gw",
        "display_name": "DEV-tier-1-gw",
        "failover_mode": "NON_PREEMPTIVE",
        "tier0_path":"/infra/tier-0s/DC-01-ENVT-01-TIER-0-GW",
        "route_advertisement_types": [
          "TIER1_CONNECTED",
          "TIER1_STATIC_ROUTES"
        ],
```

```
        "children": [
          {
           "resource_type":"ChildLocaleServices",

           "LocaleServices":{
               "resource_type":"LocaleServices",
               "id":  "default",
                "edge_cluster_path": "/infra/sites/default/enforcement-
points/default/edge-clusters/e6d88327-640b-4d33-b0b5-578b1311e7b0"
                }
        },
          {
            "resource_type": "ChildSegment",
            "Segment": {
              "resource_type": "Segment",
              "id": "DEV-RED-web-segment",
              "description": "DEV-RED-web-segment",
              "display_name": "DEV-RED-web-segment",
              "transport_zone_path": "/infra/sites/default/enforcement-
points/default/transport-zones/3a60b876-b912-400d-91b2-bdb0ef602fa0",
              "subnets": [
                {
                  "gateway_address": "10.10.1.1/24"
                }
              ]
            }
          },
          {
            "resource_type": "ChildSegment",
```

```
            "Segment": {
              "resource_type": "Segment",
              "id": "DEV-RED-app-segment",
              "description": "DEV-RED-app-segment",
              "display_name": "DEV-RED-app-segment",
              "transport_zone_path": "/infra/sites/default/enforcement-
points/default/transport-zones/3a60b876-b912-400d-91b2-bdb0ef602fa0",
              "subnets": [
                {
                  "gateway_address": "10.20.2.1/24"
                }
              ]
            }
          },
          {
            "resource_type": "ChildSegment",
            "Segment": {
              "resource_type": "Segment",
              "id": "DEV-RED-db-segment",
              "description": "DEV-RED-db-segment",
              "display_name": "DEV-RED-db-segment",
              "transport_zone_path": "/infra/sites/default/enforcement-
points/default/transport-zones/3a60b876-b912-400d-91b2-bdb0ef602fa0",
              "subnets": [
                {
                  "gateway_address": "10.20.3.1/24"
                }
              ]
            }
```

```
        },
        {
           "resource_type": "ChildPolicyNat",
           "PolicyNat": {
           "id": "USER",
           "resource_type": "PolicyNat",
           "children": [
              {
                 "resource_type": "ChildPolicyNatRule",
                 "PolicyNatRule": {
                    "resource_type": "PolicyNatRule",
                    "id": "DEV-RED-nat-rule-1",
                    "action": "SNAT",
                    "source_network": "10.10.0.0/23",
                    "service": "",
                    "translated_network": "30.30.30.20",
                    "scope": [],
                    "enabled": true,
                    "firewall_match": "BYPASS",
                    "display_name": "DEV-RED-nat-rule-1",
                    "parent_path": "/infra/tier-1s/DEV-tier-1-gw/nat/USER"
                 }
              }
           ]
        }
     }
    ]
   }
},
```

```
{
  "resource_type": "ChildDomain",
  "marked_for_delete": false,
  "Domain": {
    "id": "default",
    "resource_type": "Domain",
    "description": "default",
    "display_name": "default",
    "marked_for_delete": false,
    "children": [
      {
        "resource_type": "ChildGroup",
        "Group": {
          "resource_type": "Group",
          "marked_for_delete": false,
          "description": "DEV-RED-web-vms",
          "display_name": "DEV-RED-web-vms",
          "id": "DEV-RED-web-vms",
          "expression": [
            {
              "member_type": "VirtualMachine",
              "value": "DEVREDwebvm",
              "key": "Tag",
              "operator": "EQUALS",
              "resource_type": "Condition"
            }
          ]
        }
      },
```

```
{
  "resource_type": "ChildGroup",
  "Group": {
    "resource_type": "Group",
    "marked_for_delete": false,
    "description": "DEV-RED-app-vms",
    "display_name": "DEV-RED-app-vms",
    "id": "DEV-RED-app-vms",
    "expression": [
      {
        "member_type": "VirtualMachine",
        "value": "DEVREDappvm",
        "key": "Tag",
        "operator": "EQUALS",
        "resource_type": "Condition"
      }
    ]
  }
},
{
  "resource_type": "ChildGroup",
  "Group": {
    "resource_type": "Group",
    "description": "DEV-RED-db-vms",
    "display_name": "DEV-RED-db-vms",
    "id": "DEV-RED-db-vms",
    "expression": [
      {
        "member_type": "VirtualMachine",
```

```
          "value": "DEVREDdbvm",
          "key": "Tag",
          "operator": "EQUALS",
          "resource_type": "Condition"
        }
      ]
    }
  },
  {
    "resource_type": "ChildSecurityPolicy",
    "marked_for_delete": false,
    "SecurityPolicy": {
      "id": "DEV-RED-intra-app-policy",
      "resource_type": "SecurityPolicy",
      "description": "communication map",
      "display_name": "DEV-RED-intra-app-policy",
      "rules": [
        {
          "resource_type": "Rule",
          "description": "Communication Entry",
          "display_name": "any-to-DEV-RED-web",
          "sequence_number": 1,
          "source_groups": [
            "ANY"
          ],
          "destination_groups": [
            "/infra/domains/default/groups/DEV-RED-web-vms"
          ],
          "services": [
```

```
      "/infra/services/HTTPS"
    ],
    "action": "ALLOW"
  },
  {
    "resource_type": "Rule",
    "description": "Communication Entry 2",
    "display_name": "DEV-RED-web-to-app",
    "sequence_number": 2,
    "source_groups": [
      "/infra/domains/default/groups/DEV-RED-web-vms"
    ],
    "destination_groups": [
      "/infra/domains/default/groups/DEV-RED-app-vms"
    ],
    "services": [
      "/infra/services/HTTP"
    ],
    "action": "ALLOW"
  },
  {
    "resource_type": "Rule",
    "description": "Communication Entry 3",
    "display_name": "DEV-RED-app-to-db",
    "sequence_number": 2,
    "source_groups": [
      "/infra/domains/default/groups/DEV-RED-app-vms"
    ],
    "destination_groups": [
```

```
            "/infra/domains/default/groups/DEV-RED-db-vms"
          ],
          "services": [
            "/infra/services/MySQL"
          ],
          "action": "ALLOW"
        }
      ]
    }
  },
  {
    "resource_type": "ChildGatewayPolicy",
    "marked_for_delete": false,
    "GatewayPolicy": {
      "resource_type": "GatewayPolicy",
      "id": "DEV-RED-section",
      "display_name": "DEV-RED-section",
      "parent_path": "/infra/domains/default",
      "marked_for_delete": false,
      "rules": [
        {
         "source_groups": [
                "ANY"
          ],
          "destination_groups": [
              "/infra/domains/default/groups/DEV-RED-web-vms"
          ],
          "services": [
              "/infra/services/HTTPS"
```

```
    ],
    "profiles": [
        "ANY"
    ],
    "action": "ALLOW",
    "logged": false,
    "scope": [
        "/infra/tier-1s/DEV-tier-1-gw"
    ],
    "disabled": false,
    "notes": "",
    "direction": "IN_OUT",
    "tag": "",
    "ip_protocol": "IPV4_IPV6",
    "resource_type": "Rule",
    "id": "Any-to-web",
    "display_name": "Any-to-web"
},
                {
 "source_groups": [
        "ANY"
    ],
    "destination_groups": [
        "/infra/domains/default/groups/DEV-RED-web-vms",
        "/infra/domains/default/groups/DEV-RED-app-vms",
        "/infra/domains/default/groups/DEV-RED-db-vms"
    ],
    "services": [
        "ANY"
```

```
                ],
                "profiles": [
                    "ANY"
                ],
                "action": "DROP",
                "logged": false,
                "scope": [
                    "/infra/tier-1s/DEV-tier-1-gw"
                ],
                "disabled": false,
                "notes": "",
                "direction": "IN_OUT",
                "tag": "",
                "ip_protocol": "IPV4_IPV6",
                "resource_type": "Rule",
                "id": "DenyAny",
                "display_name": "DenyAny"
              }
             ]
          }
        }
    ]
  }
},
  {
    "resource_type": "ChildLBClientSslProfile",
    "marked_for_delete": false,
    "LBClientSslProfile": {
      "resource_type": "LBClientSslProfile",
```

```
      "id": "batchSetupClientSslProfile",
      "cipher_group_label": "CUSTOM",
      "session_cache_enabled": true,
      "ciphers": [
        "TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256",
        "TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384"
      ],
      "protocols": [
        "TLS_V1_2"
      ]
    }
  },
  {
    "resource_type": "ChildLBServerSslProfile",
    "marked_for_delete": false,
    "LBServerSslProfile": {
      "resource_type": "LBServerSslProfile",
      "id": "batchSetupServerSslProfile",
      "cipher_group_label": "CUSTOM",
      "session_cache_enabled": true,
      "ciphers": [
        "TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256",
        "TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384"
      ],
      "protocols": [
        "TLS_V1_2"
      ]
    }
  },
```

```
{
  "resource_type": "ChildLBAppProfile",
  "marked_for_delete": false,
  "LBAppProfile": {
    "resource_type": "LBHttpProfile",
    "id": "batchSetupHttpAppProfile",
    "x_forwarded_for": "INSERT"
  }
},
{
  "resource_type": "ChildLBMonitorProfile",
  "marked_for_delete": false,
  "LBMonitorProfile": {
    "resource_type": "LBHttpMonitorProfile",
    "marked_for_delete": false,
    "id": "batchSetupHttpMonitor1",
    "monitor_port": 80,
    "timeout": 5,
    "response_status_codes": [
      200,
      300
    ]
  }
},
{
  "resource_type": "ChildLBMonitorProfile",
  "marked_for_delete": false,
  "LBMonitorProfile": {
    "resource_type": "LBHttpsMonitorProfile",
```

```
      "id": "batchSetupHttpsMonitor1",
      "monitor_port": 443,
      "timeout": 5,
      "response_status_codes": [
        200
      ]
    }
  },
  {
    "resource_type": "ChildLBService",
    "marked_for_delete": false,
    "LBService": {
      "resource_type": "LBService",
      "id": "DEV-RED-LbService",
      "connectivity_path": "/infra/tier-1s/DEV-tier-1-gw",
      "error_log_level": "DEBUG",
      "access_log_enabled": true
    }
  },
  {
    "resource_type": "ChildLBVirtualServer",
    "marked_for_delete": false,
    "LBVirtualServer": {
      "resource_type": "LBVirtualServer",
      "id": "DEV-RED-VirtualServer1",
      "lb_service_path": "/infra/lb-services/DEV-RED-LbService",
      "ip_address": "30.10.200.1",
      "ports": [
        "443"
```

```
    ],
    "pool_path": "/infra/lb-pools/DEV-RED-web-Pool",
    "application_profile_path": "/infra/lb-app-profiles/batchSetupHttpAppProfile",
    "client_ssl_profile_binding": {
      "ssl_profile_path": "/infra/lb-client-ssl-profiles/batchSetupClientSslProfile",
      "default_certificate_path": "/infra/certificates/batchSslSignedCertDEV-RED",
      "client_auth_ca_paths": [
        "/infra/certificates/batchSslCACertDEV-RED"
      ],
      "certificate_chain_depth": 2
    },
    "server_ssl_profile_binding": {
      "ssl_profile_path": "/infra/lb-server-ssl-profiles/batchSetupServerSslProfile",
      "server_auth": "IGNORE",
      "client_certificate_path": "/infra/certificates/batchSslSignedCertDEV-RED",
      "server_auth_ca_paths": [
        "/infra/certificates/batchSslCACertDEV-RED"
      ],
      "certificate_chain_depth": 2
    }
  }
},
{
  "resource_type": "ChildLBPool",
  "marked_for_delete": false,
  "LBPool": {
    "id": "DEV-RED-web-Pool",
    "resource_type": "LBPool",
    "marked_for_delete": false,
```

```
    "active_monitor_paths": [
      "/infra/lb-monitor-profiles/batchSetupHttpsMonitor1"
    ],
        "algorithm": "ROUND_ROBIN",
        "member_group": {
            "group_path": "/infra/domains/default/groups/DEV-RED-web-vms",
            "ip_revision_filter": "IPV4"
        },
        "snat_translation": {
            "type": "LBSnatDisabled"
        }
  }
},
{
  "resource_type": "ChildLBVirtualServer",
  "marked_for_delete": false,
  "LBVirtualServer": {
    "resource_type": "LBVirtualServer",
    "id": "DEV-RED-VirtualServer2",
    "lb_service_path": "/infra/lb-services/DEV-RED-LbService",
    "ip_address": "10.10.200.1",
    "ports": [
      "80"
    ],
    "pool_path": "/infra/lb-pools/DEV-RED-app-Pool",
    "application_profile_path": "/infra/lb-app-profiles/batchSetupHttpAppProfile"
  }
},
{
```

```
      "resource_type": "ChildLBPool",
      "marked_for_delete": false,
      "LBPool": {
        "id": "DEV-RED-app-Pool",
        "resource_type": "LBPool",
        "marked_for_delete": false,
        "active_monitor_paths": [
          "/infra/lb-monitor-profiles/batchSetupHttpMonitor1"
        ],
            "algorithm": "ROUND_ROBIN",
            "member_group": {
                "group_path": "/infra/domains/default/groups/DEV-RED-app-vms",
                "ip_revision_filter": "IPV4"
            },
            "snat_translation": {
                "type": "LBSnatDisabled"
            }
      }
    },
        {
      "resource_type": "ChildTlsTrustData",
      "marked_for_delete": false,
      "TlsTrustData": {
        "resource_type": "TlsTrustData",
        "marked_for_delete": false,
        "id": "batchSslCACertDEV-RED",
        "pem_encoded": "-----BEGIN CERTIFICATE-----
\nMIIExTCCA62gAwIBAgIBADANBgkqhkiG9w0BAQUFADB9MQswCQYDVQQGEwJFVTEn\nMCUGA1UEChMeQUMgQ2FtZ
XJmaXJtYSBTQSBDSUYgQTgyNzQzMjg3MSMwIQYDVQQL\nExpodHRwOi8vd3d3LmNoYW1iZXJzaWduLm9yZzEgMB4G
A1UEAxMXR2xvYmFsIENo\nYW1iZXJzaWduIFJvb3QwHhcNMDMwOTMwMTYxNDE4WhcNMzcwOTMwMTYxNDE4WjB9\nM
```

QswCQYDVQQGEwJFVTEnMCUGA1UEChMeQUMgQ2FtZXJmaXJtYSBTQSBDSUYgQTgy\nNzQzMjg3MSMwIQYDVQQLExpo
dHRwOi8vd3d3LmNoYW1iZXJzaWduLm9yZzEgMB4G\nA1UEAxMXR2xvYmFsIENoYW1iZXJzaWduIFJvb3QwggEgMA0
GCSqGSIb3DQEBAQUA\nA4IBDQAwggEIAoIBAQCicKLQn0KuWxfH2H3PFIP8T8mhtxOviteePgQKkotgVvq0\nMi+I
TaFgCPS3CU6gSS9J1tPfnZdan5QEcOw/Wdm3zGaLmFIoCQLfxS+EjXqXd7/s\nQJ0lcqu1PzKY+7e3/HKE5TWH+VX
6ox8Oby4o3Wmg2UIQxvi1RMLQQ3/bvOSiPGpV\neAp3qdjqGTK3L/5cPxvusZjsyq16aUXjlg9V9ubtdepl6DJWk0
aJqCWKZQbua795\nB9Dxt6/tLE2Su8CoX6dnfQTyFQhwrJLWfQTSM/tMtgsL+xrJxI0DqX5c8lCrEqWh\nz0hQpe/
SyBoT+rB/sYIcd2oPX9wLlY/vQ37mRQklAgEDo4IBUDCCAUwwEgYDVR0T\nAQH/BAgwBgEB/wIBDDA/BgNVHR8EOD
A2MDSgMqAwhi5odHRwOi8vY3JsLmNoYW1i\nZXJzaWduLm9yZy9jaGFtYmVyc2lnbnJvb3QuY3JsMB0GA1UdDgQWB
BRDnDafsJ4w\nTcbOX60Qq+UDpfqpFDAOBgNVHQ8BAf8EBAMCAQYwEQYJYIZIAYb4QgEBBAQDAgAH\nMCoGA1UdEQ
QjMCGBH2NoYW1iZXJzaWducm9vdEBjaGFtYmVyc2lnbi5vcmcwKgYD\nVR0SBCMwIYEfY2hhbWJlcnNpZ25yb290Q
GNoYW1iZXJzaWduLm9yZzBbBgNVHSAE\nVDBSMFAGCysGAQQBgYcuCgEBMEEwPwYIKwYBBQUHAgEWM2h0dHA6Ly9j
cHMuY2hh\nbWJlcnNpZ24ub3JnL2Nwcy9jaGFtYmVyc2lnbnJvb3QuaHRtbDANBgkqhkiG9w0B\nAQUFAAOCAQEAP
DtwkfkEVCeR4e3t/mh/YV3lQWVPMvEYBZRqHN4fcNs+ezICNLUM\nbKGKfKX0j//U2K0X1S0E0T9YgOKBWYi+wONG
kyT+kL0mojAt6JcmVzWJdJYY9hXi\nryQZVgICsroPFOrGimbBhkVVi76SvpykBMdJPJ7oKXqJ1/6v/2j1pReQvay
ZzKWG\nVwlnRtvWFsJG8eSpUPWP0ZIV018+xgBJOm5YstHRJw0lyDL4IBHNfTIzSJRUTN3c\necQwn+uOuFW114hc
xWokPbLTBQNRxgfvzBRydD1ucs4YKIxKoHflCStFREest2d/\nAYoFWpO+ocH/+OcOZ6RHSXZddZAa9SaP8A==\n-
----END CERTIFICATE-----\n"

```
      }
    },
    {
      "resource_type": "ChildTlsTrustData",
      "marked_for_delete": false,
      "TlsTrustData": {
        "resource_type": "TlsTrustData",
        "marked_for_delete": false,
        "id": "batchSslSignedCertDEV-RED",
```

"pem_encoded": "-----BEGIN CERTIFICATE-----
\nMIIE7zCCAtegAwIBAgICEAEwDQYJKoZIhvcNAQEFBQAwezELMAkGA1UEBhMCVVMx\nCzAJBgNVBAgMAkNBMQswC
QYDVQQHDAJQQTEPMA0GA1UECgwGVk13YXJlMQ0wCwYD\nVQQLDAROU0JVMQ4wDAYDVQQDDAVWaXZlazEiMCAGCSqG
SIb3DQEJARYTdnNhcmFv\nZ2lAdm13YXJlLmNvbTAeFw0xNDA4MDYyMTE1NThaFw0xNTA4MDYyMTE1NThaMG4x\nC
zAJBgNVBAYTAlVTMQswCQYDVQQIEwJDQTEPMA0GA1UEChMGVk13YXJlMQ0wCwYD\nVQQLEwROU0JVMQ4wDAYDVQQD
EwVWaXZlazEiMCAGCSqGSIb3DQEJARYTdnNhcmFv\nZ2lAdm13YXJlLmNvbTCCASIwDQYJKoZIhvcNAQEBBQADggE
PADCCAQoCggEBANHv\nl6nlZEbY+PamrPYxiit3jlYY7tIOUtLNqYtANBMTNVuCQweREHCNIXmsDGDvht28\nTZm0
RwO7U72ZMlUYIM9JeDKvf4SwpGyXEyCCPsrnV4ZWaazLDS+rsi0daO2ak70+\nc9pnfGIogf/tcslFUb//dsK3wJQ
cirq3Aii/Eswzva6tiP4TOjAA8Ujy1eLmnQVN\nIXpAeAqRmk+AKfzXS+fRjeaMQsZD0rySJ1Q2M//Y0/e9nTLUx4
50rIAlx/EfwhNJ\nHkNh5hCsblaCv9bUiIkIuDBiNn2zh3hUmRo/gjk94lSoG6plILOM8BY1Ro5uSqyu\nRSrJXzc

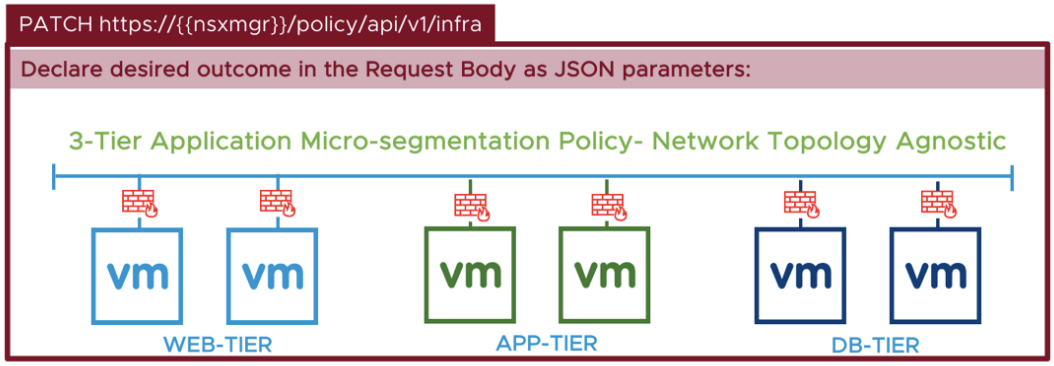
OQ1ndmXjCxKUCAwEAAaOBiTCBhjAJBgNVHRMEAjAAMAsGA1UdDwQEAwIF\n4DAsBglghkgBhvhCAQ0EHxYdT3Blbl
NTTCBHZW5lcmF0ZWQgQ2VydGlmaWNhdGUw\nHQYDVR0OBBYEFCKOu6UTn7XsNQVQxOpOUzOc9Yh3MB8GA1UdIwQYM
BaAFOqoDj0V\n7pC6BhIjy3sVV73EfBZMMA0GCSqGSIb3DQEBBQUAA4ICAQClSkVbIb3HEJNBaRBW\nnm9cf+iU9l
pMCYdQAsYAeE9ltSbfJMw8e+Yla+m8D4ZGSLzevjEyTHslACd7666q\nTBviPSlopYkMmiiwaGpTVL8qIhhxzkMOM
ea4AiPgZ4FUDzb/yYKGSQEIE3/5MMbP\nvUEac+n0JIiwHZZP4TgT7vPD9so2cc6dZU0CW+vTu+50zzsOUKUYAfUk
k6k5SL6H\nkho+cavL38Dyjx2DdvZ/dtZkommbj+wtoluRR17wTwSD1yCqpfPAvGwbSwUwX2U+\nwEqGQsnfBYsls
f81PNPzVDAsE5asf5dooOmx9LogbzVT7B27VAfcpqtaT5WH6jij\nusVzUaRVlylZHGqXQ3QeYFG4zulT4q2V9Q/C
VnX8uOzRFIcgAyYkizd603EgMWPq\nAyEqu5HTeqomk+cwsyel35q9QpGl8iDjJQaCZNW7tTPobVWYcdt7VA1i0Mt
nNz4R\nxjb+3WKPTswawKqO1souuXpBiGptMKjb/gasDh2gH+MvGob+9XQ0HkKUvDUeaU5a\n+JdASpSsKswIx6rA
saIvNREXh3ur8ao3DEBpo/og5qNhZmnTBKcDLElgIRMjF0GD\nT0ycWSV33x4X3U+qogXOr7mAVIKBWEp/w2JeCRF
bLKxLc4q7CESaYRWGSml0McmH\n0tmEO4++tc1WSc2i/WGJYsZbHA==\n-----END CERTIFICATE-----\n-----
BEGIN CERTIFICATE-----
\nMIIF1jCCA76gAwIBAgIJANY0bE9WZ1GVMA0GCSqGSIb3DQEBBQUAMHsxCzAJBgNV\nBAYTAlVTMQswCQYDVQQID
AJDQTELMAkGA1UEBwwCUEExDzANBgNVBAoMBlZNd2Fy\nZTENMAsGA1UECwwETlNCVTEOMAwGA1UEAwwFVml2ZWsx
IjAgBgkqhkiG9w0BCQEW\nE3ZzYXJhb2dpQHZtd2FyZS5jb20wHhcNMTQwNzE2MTgwMjQ4WhcNMjQwNzEzMTgw\nM
jQ4WjB7MQswCQYDVQQGEwJVUzELMAkGA1UECAwCQ0ExCzAJBgNVBAcMAlBBMQ8w\nDQYDVQQKDAZWTXdhcmUxDTAL
BgNVBAsMBE5TQlUxDjAMBgNVBAMMBVZpdmVrMSIw\nIAYJKoZIhvcNAQkBFhN2c2FyYW9naUB2bXdhcmUuY29tMII
CIjANBgkqhkiG9w0B\nAQEFAAOCAg8AMIICCgKCAgEA3bvIkxqNzTEOSlWfMRPCKUt2hy064GP3OwR8tXqf\n0Pem
yT/2SgVFPtAVv3dH7qBG+CmnYXlSymgHrVb8d9Kh08Jv+utkunQmGqecUjcd\nt0ziJj+aZQx6yxfOOwmYxXjVbKR
gtLFby30KgFKJ1/xC45bNGzEI99u3ZFrEfkwl\n0ebozdB6Tfjo/ZzsbtuwqGcgfWMwFqI9P/8upn7rzBTHXp4Z8z
ygf1+/fkIxUu9o\n5Q/E1cjaLrKBa9ETMSmpXenEQdQvT2vmj69fafvXbBA+2nZPO/6Hmhgnbni+qglM\n0h7BUpf
/NXb7vybTFRhm1EO2dhQnK0IHU8qeEgxt/vyuD4JlBsUw/HqD3XJ20Qj2\nulOoRa8cQdIuDX/0gLJ92g2kCKTEE7
iHa5jDdba7MqUQvOxJPJ4Mi55iuiolh88o\ne92jhS2zxImcy/IElXLxwJyWv0WUxQNX+0h+lafK9XPsZIV3K+W7P
PpMvymjDNIC\nVbjvURDaHg/uRszZovfFewiIvYCR4jB5eCud4vOLY1iLyEt2CnmTCPH9No1lk2B/\n1Ej/QJOPFJ
C/wbDeTiTg7sgJIdTHcRMdumIMhtQHTYYXxd3u3Oy7M9fxYCnHQE14\nejh4/37Qn1bylOqACVT0u++pamlT1fc70
Y1Bwq5xS/OJGRmK0FAHiWus/3QvV9Kj\nUucCAwEAAaNdMFswHQYDVR0OBBYEFOqoDj0V7pC6BhIjy3sVV73EfBZM
MB8GA1Ud\nIwQYMBaAFOqoDj0V7pC6BhIjy3sVV73EfBZMMAwGA1UdEwQFMAMBAf8wCwYDVR0P\nBAQDAgEGMA0GC
SqGSIb3DQEBBQUAA4ICAQCFD6o1SALwTxAMmHqt6rrwjZdrUMLe\n0vZ1lsjlr82MrUk9L1YOsSFRFGLpYMhmIC/p
daziMxEOI+RifRSI9sk/sY3XlsrL\nuI/92sE9qLV6/PGZsaHYeQcDduaqLqHj7LnsCkgoVZqYhpgpRvgiuUm8faW
W9piG\nO0t/PuKpyxWRn+0dqzsH+Nhr/lMoYPqeURphphqiiqoTGcmREEYrDC+MoUsTeHy4\nPy2NNCB5J5qQpMfw
fWBeLf0dXXpFk7ggF0dHW/Ma/b8g+fdVE6AswY3NG6TV8phy\nOoNCgqIIO18OuFVL2DnYDoDaEjin/Y5l6U32BAs
iCTyiUrCr4+4V7Awa10ipZiPK\niQlIs0vbXD9tSyiP1yTn3tXXHE7OZnT5nE1//UQbEaQWbQcgZOCoH54M7m03aM
S5\n1PHs9BHt7zj3ASDF682rsiZTKgW+hv6TTTdfgDHMEO5+ocpIXKAeN9Kx3XSp6jHt\n5yMT2IUv3BEO9i+Dj8C
BwvUHU9keinWCJ3i8WbiVhDsQoSnIARX51pmZ9Hz+JelS\nCh0BJtJsWac0Ceq5u62qzRNCj2D6ZqWHjmlzJ4Wnvc
QMRYxrskct4kS/zX4NTZyx\nlBH6xjE5pnf45jUWkiAD9IfGC40bApHorgC/2wCCTmkL8nxIGY1jg1zHXO/cxTxp\
nVcf1BfHFyi5CjA==\n-----END CERTIFICATE-----\n",

"private_key": "-----BEGIN RSA PRIVATE KEY-----
\nMIIEpAIBAAKCAQEA0e+XqeVkRtj49qas9jGKK3eOVhju0g5S0s2pi0A0ExM1W4JD\nB5EQcI0heawMYO+G3bxNm
bRHA7tTvZkyVRggz0l4Mq9/hLCkbJcTIII+yudXhlZp\nrMsNL6uyLR1o7ZqTvT5z2md8YiiB/+1yyUVRv/92wrfA

```
lByKurcCKL8SzDO9rq2I\n/hM6MADxSPLV4uadBU0hekB4CpGaT4Ap/NdL59GN5oxCxkPSvJInVDYz/9jT972d\nM
tTHjnSsgCXH8R/CE0keQ2HmEKxuVoK/1tSIiQi4MGI2fbOHeFSZGj+COT3iVKgb\nqmUgs4zwFjVGjm5KrK5FKslf
Nw5DWd2ZeMLEpQIDAQABAoIBAQCBp4I4WEa9BqWD\n11580g2uWLEcdVuReW0nagLq0GUY3sUWVfXFx46qpE7nUR1
4BJZ7fR9D7TXqlRfb\nwbB3I2an/ozwaLjNnzZ9JjSW4DmdoJDKk7XCFMl5BoYNHNu/2rahqt9sJHuKN9BJ\n2kEJ
EvmxJToYednC33nCZOI9ffxDBhZKN1krnHjouI56MZv23e06+cwwjrFUnIPI\nNNfkTTqDMU/xj5xmltrWhZIr/RP
ogLS4kdwRS8Q8pPvJOXQlg7+imrDxg7MckMgb\nE73uJv5sfhbsxgn9d8sYVhD9lwbb+QpXUro8f5XzVFwMpRFbDT
hGE0eQx7ULCWZz\n+2+/x+jFAoGBAPqDfU/EBHVBF/O0JnVFC7A26ihQUQIqUu2N3oGi/L+io2uIw8Cd\n9eHuxmw
I2DPJ5KlRz7i1ZeGlZoRNN7dt3p7NhKT4O+7hyBVMDItubKkwdg2rULj6\nz9iShtKomzyZaSDA8VbNZX/qgDM7Uf
lKcvXUA41UuJGrgiJmm3DZTqqLAoGBANaI\nml2NB6aFnd/4PN1XKZzFibS1DvcnooX+LPtR6+ky/0wst7DXF1qnp
3XWVG6R86ci\nCFoTNsleryrFmKnY5oUl41EcNqpnVGU1+lth6rl4LnVL9GwtiU2h9kV5p7w0ExRk\nkVjvE4K8f8
w5eDcO39QogkD0AYXpN1pj9l6EEaOPAoGAT0kqcgJx/sJZWFJeEaOG\nrYDT32p8GRlYIcNS9uik4eoRmskwW1gjK
BywRCUQeGOfsU8pVSZkVmRI6/qcdbua\nR9x37NZ78YEYGFV3avHKBkpGMtFTvRf0jHDjpuyiJS3QrgMi3vwm8bNA
W/acXTAI\n7nDppuN3fvMvPsAG1lKQqT0CgYAJIF6QxEMjDmQc9w5/zAl1JeIp0doFIaaEVL/N\nITsL/KNnti9KU
pwnuyIgnTGSUpsu7P+19UNLZb/F7goEj7meyHHXLYAV17d7ZsRz\nxsKZiUdQrh6Dy5wftVgotHgyRXTaVTzpr6IA
2cwGABvhG7zh5adE5Bx8eeNk8QO2\nGaA2eQKBgQDnpBPL0OtVcva1gOIeS41Kaa78/VxN64fKCdkJNfwr9NUz51u
6RMrh\nc2zWaTp3QG062zhdSuUATVJ9kK/NgVT9Afmb21H76xE9KY3fztb1SqRCZGMjHeEr\n563mDimPiOPUATWX
yZS5/HQSLIRLjJ9+mfBFVFEgFNGK55pOmyMTaQ==\n-----END RSA PRIVATE KEY-----\n",

        "key_algo": "RSA"

      }

    }

  ]

}'
```


8.2. Example 2: Life Cycle of Security Configuration

This example demonstrates how a security admin can leverage the declarative API to manage life cycle of security configuration. The following diagram shows the entire application topology and the desired outcome to provide zero trust security model for an application:



The below API can be used to deploy the exact security policy across multiple systems:

```
curl -X PATCH \
  https:// nsx-appliance.mylab.net /policy/api/v1/infra/ \
  -H 'authorization: Basic YWRtaW46Vk13YXJlIW1ncjE5akg=' \
  -H 'cache-control: no-cache' \
  -H 'content-type: application/json' \
  -d '{
  "resource_type": "Infra",
  "children": [
    {
      "resource_type": "ChildDomain",
      "marked_for_delete": false,
      "Domain": {
        "id": "default",
        "resource_type": "Domain",
        "description": "default",
        "display_name": "default",
        "children": [
          {
            "resource_type": "ChildGroup",
            "marked_for_delete": false,
            "Group": {
              "resource_type": "Group",
              "description": "DEV-RED-web-vms",
              "display_name": "DEV-RED-web-vms",
              "id": "DEV-RED-web-vms",
              "expression": [
                {
```

```
        "member_type": "VirtualMachine",
        "value": "DEVREDwebvm",
        "key": "Tag",
        "operator": "EQUALS",
        "resource_type": "Condition"
      }
    ]
  }
},
{
  "resource_type": "ChildGroup",
  "marked_for_delete": false,
  "Group": {
    "resource_type": "Group",
    "description": "DEV-RED-app-vms",
    "display_name": "DEV-RED-app-vms",
    "id": "DEV-RED-app-vms",
    "expression": [
      {
        "member_type": "VirtualMachine",
        "value": "DEVREDappvm",
        "key": "Tag",
        "operator": "EQUALS",
        "resource_type": "Condition"
      }
    ]
  }
},
{
```

```
    "resource_type": "ChildGroup",
    "marked_for_delete": false,
    "Group": {
      "resource_type": "Group",
      "description": "DEV-RED-db-vms",
      "display_name": "DEV-RED-db-vms",
      "id": "DEV-RED-db-vms",
      "expression": [
        {
          "member_type": "VirtualMachine",
          "value": "DEVREDdbvm",
          "key": "Tag",
          "operator": "EQUALS",
          "resource_type": "Condition"
        }
      ]
    }
  },
  {
    "resource_type": "ChildSecurityPolicy",
    "marked_for_delete": false,
    "SecurityPolicy": {
      "id": "DEV-RED-intra-tier-1",
      "resource_type": "SecurityPolicy",
      "description": "communication map",
      "display_name": "DEV-RED-intra-tier-1",
      "category": "Environment",
      "rules": [
        {
```

```
    "resource_type": "Rule",
    "description": "Communication Entry",
    "display_name": "DEV-RED-web-to-DEV-RED-web",
    "sequence_number": 1,
    "source_groups": [
      "/infra/domains/default/groups/DEV-RED-web-vms"
    ],
    "destination_groups": [
      "/infra/domains/default/groups/DEV-RED-web-vms"
    ],
    "services": [
      "Any"
    ],
    "action": "ALLOW",
    "scope": [
      "/infra/domains/default/groups/DEV-RED-web-vms"
    ]
  },
  {
    "resource_type": "Rule",
    "description": "Communication Entry 2",
    "display_name": "DEV-RED-intra-tier-2",
    "sequence_number": 2,
    "source_groups": [
      "/infra/domains/default/groups/DEV-RED-app-vms"
    ],
    "destination_groups": [
      "/infra/domains/default/groups/DEV-RED-app-vms"
    ],
```

```
      "services": [
        "ANY"
      ],
      "action": "ALLOW",
      "scope": [
        "/infra/domains/default/groups/DEV-RED-app-vms"
      ]
    },
    {
      "resource_type": "Rule",
      "description": "Communication Entry 3",
      "display_name": "DEV-RED-intra-tier-3",
      "sequence_number": 3,
      "source_groups": [
        "/infra/domains/default/groups/DEV-RED-db-vms"
      ],
      "destination_groups": [
        "/infra/domains/default/groups/DEV-RED-db-vms"
      ],
      "services": [
        "Any"
      ],
      "action": "ALLOW",
      "scope": [
        "/infra/domains/default/groups/DEV-RED-db-vms"
      ]
    }
  ]
}
```

```
},
          {
  "resource_type": "ChildSecurityPolicy",
  "marked_for_delete": false,
  "SecurityPolicy": {
    "id": "DEV-RED-intra-app-policy",
    "resource_type": "SecurityPolicy",
    "description": "communication map",
    "display_name": "DEV-RED-intra-app-policy",
    "category": "Application",
    "rules": [
      {
        "resource_type": "Rule",
        "description": "Communication Entry",
        "display_name": "any-to-DEV-RED-web",
        "sequence_number": 1,
        "source_groups": [
          "ANY"
        ],
        "destination_groups": [
          "/infra/domains/default/groups/DEV-RED-web-vms"
        ],
        "services": [
          "/infra/services/HTTPS"
        ],
        "action": "ALLOW",
        "scope": [
          "/infra/domains/default/groups/DEV-RED-web-vms"
        ]
```

```
},
{
  "resource_type": "Rule",
  "description": "Communication Entry 2",
  "display_name": "DEV-RED-web-to-app",
  "sequence_number": 2,
  "source_groups": [
    "/infra/domains/default/groups/DEV-RED-web-vms"
  ],
  "destination_groups": [
    "/infra/domains/default/groups/DEV-RED-app-vms"
  ],
  "services": [
    "/infra/services/HTTP"
  ],
  "action": "ALLOW",
  "scope": [
    "/infra/domains/default/groups/DEV-RED-web-vms",
    "/infra/domains/default/groups/DEV-RED-app-vms"
  ]
},
{
  "resource_type": "Rule",
  "description": "Communication Entry 3",
  "display_name": "DEV-RED-app-to-db",
  "sequence_number": 3,
  "source_groups": [
    "/infra/domains/default/groups/DEV-RED-app-vms"
  ],
```

```
    "destination_groups": [
      "/infra/domains/default/groups/DEV-RED-db-vms"
    ],
    "services": [
      "/infra/services/MySQL"
    ],
    "action": "ALLOW",
    "scope": [
      "/infra/domains/default/groups/DEV-RED-db-vms",
      "/infra/domains/default/groups/DEV-RED-app-vms"
    ]
  },
  {
    "resource_type": "Rule",
    "description": "Communication Entry 4",
    "display_name": "DEV-RED-deny-any",
    "sequence_number": 4,
    "source_groups": [
      "ANY"
    ],
    "destination_groups": [
      "ANY"
    ],
    "services": [
      "ANY"
    ],
    "action": "DROP",
    "scope": [
      "/infra/domains/default/groups/DEV-RED-db-vms",
```

```
                    "/infra/domains/default/groups/DEV-RED-app-vms",
                    "/infra/domains/default/groups/DEV-RED-web-vms"
                  ]
                }
              ]
            }
          }
        ]
      }
    }
  ]
}'
```

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com.