Arista ZTX Traffic Mapper

Software Deployment Guide

Table of contents

Introduction

The Arista ZTX Traffic Mapper product family empowers Arista Multi-domain Segmentation Services (MSS) solutions with a traffic mapping service that is used to generate precise and granular Zero Trust policies, and to accurately identify policy violations.

This document discusses network design best practices and provides a set of validated network configuration examples that network administrators and architects can use as a reference when deploying the Arista ZTX Traffic Mapper as part of a MSS solution.

The Arista ZTX Traffic Mapper product family includes EOS-based appliances like the Arista ZTX-7250S (physical appliance or ZTX) and the Arista vZTX (virtual appliance or vZTX). For simplicity most of the examples and figures in this guide reference the physical appliance for capabilities that are common to both ZTX and vZTX, and when applicable, it mentions specific differences that apply exclusively to the virtual or physical appliance. Below is a comparison table that summarizes the differences and similarities in deploying the ZTX and the vZTX appliances, with references to corresponding chapters of this guide.

Deployment Module	ZTX	vZTX
Traffic Mapper Profile	Not required (pre-configured setting)	Required
Out-of-band Connectivity	Management interface with default or management VRF	
In-band Physical Connectivity Options	Centralized and Distributed topology	Dual-homed topology
In-band Link Aggregation Option	Yes	No
In-band Layer-3 Connectivity Options	Static or Dynamic routing over link aggregation	Static or Dynamic routing over routed ports
L2oGRE Tunnel Provisioning	Automatic, using Loopback or SVI address	Automatic, using Loopback address
Managing Traffic Mapper objects and functions	CloudVision onboarding and MSS Service Studio	

Definitions and acronyms

The following table defines in alphabetical order the technical terms and acronyms used throughout this document.

Technical term	Description
BGP	Border Gateway Protocol
CLI	Command Line Interface
EOS	Arista Extensible Operating System (EOS) is a Linux-based network operating system (NOS) that powers Arista's cloud networking solutions. It's designed to be programmable and resilient, and is used in data centers, campuses, and carrier networks
Ethernet	Ethernet is the most prevalent layer-2 protocol
IANA	Internet Assigned Numbers Authority
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol is the most prevalent layer-3 protocol
L2oGRE	Layer-2 over Generic Routing Encapsulation is an IP protocol for transparently tunneling layer-2 packets over a layer-3 network
Lateral vs Vertical or E-W vs N-S	In the context of enterprise networks, Vertical or North-South indicates the communication between enterprise endpoints and external resources reachable over the public internet network or located in remote corporate sites or in a different security zone. It contrasts with Lateral or East-West communication that indicates communication patterns inside the corporate network within the same security zone.
layer-2	Data-link layer in OSI model
layer-3	Network layer in OSI model
layer-4	Transport layer in OSI model
NTP	Network Time Protocol
OSI	Open Systems Interconnection model for network communication

Technical term	Description
OSPF	Open Shortest Path First protocol
SR-IOV	Single Root Input/Output Virtualization is a virtualization technology that increases the manageability and throughput performance of physical network adapters
SVI	Switched Virtual Interface, also called VLAN Interface, is a configuration construct applied to a VLAN that includes layer-3 properties like an IP address or a VRF. It is primarily used to connect a layer-3 interface to a VLAN in order to provide inter-VLAN communication
Security Domain	A collection of physical switches that constitutes a Zero Trust network enforcement function and share MSS objects like policies and groups
vEOS	Arista Virtual EOS is an EOS software package that can be deployed as a virtual machine in different hypervisors and leverages network forwarding technologies like SR-IOV
VLAN	Virtual Local Area Network is a layer-2 ethernet segmentation construct defined by [IEEE 802.1Q standard]
VRF	Virtual Routing and Forwarding is a layer-3 segmentation technology that allows multiple instances of a routing table to co-exist within the same router. In MSS context, the VRF identifier can be used to represent a security zone, even in cases where routing is inactive.
Whitelist	An explicit list or register of entities that are trusted to receive access to a particular service or resource

Role of Arista ZTX Traffic Mapper in a Zero Trust network

Zero Trust is a security model founded on the principle that trusted communication is always granted explicitly with precise whitelist rules that must be continually evaluated: Arista MSS technology provides two functions to achieve this goal:

1. The ability to dynamically classify the enterprise devices in security **micro-perimeters** zones, called **groups** or tags, that are smaller than traditional network segmentation constructs, where lateral communication can be granularly controlled.
2. A **traffic mapping service** to continuously evaluate stateful communication inside an Arista network, which can be combined with the previous function (1) to generate precise and granular Zero Trust policy rules that match actual legitimate traffic.

The Arista ZTX Traffic Mapper is the component of the MSS solution that provides the traffic mapping data to the traffic mapping service. The traffic mapping service data and the micro-perimeter groups data are ingested by Arista CloudVision in its powerful Network Data Lake backend, and, as represented by the following diagram, are selectively used by the MSS Policy Builder function to generate rule recommendations:

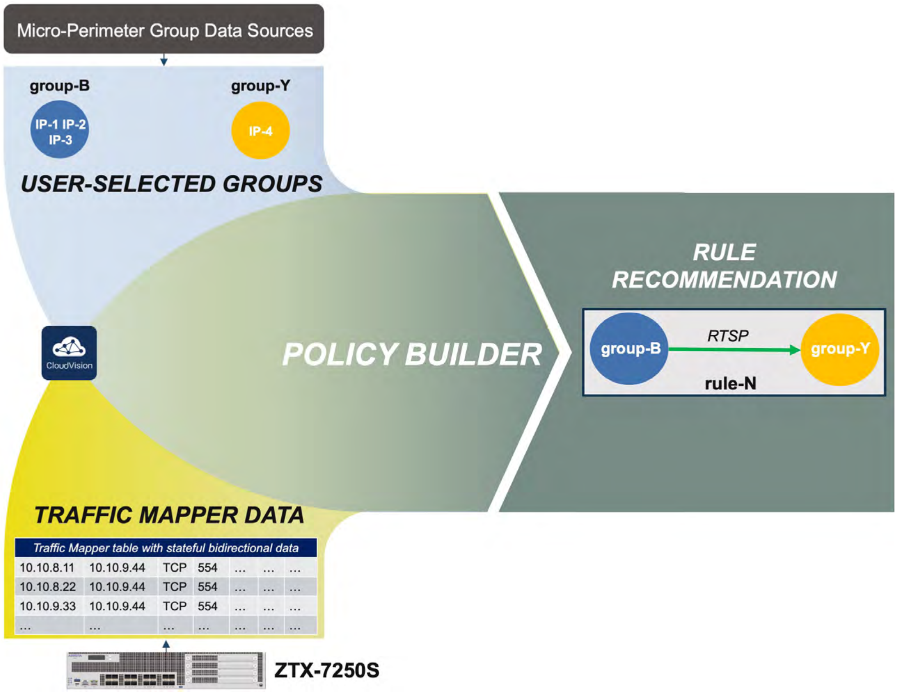


Fig.1 MSS Policy Builder logical block diagram.

Deployment of the ZTX Traffic Mapper in an Arista network

This chapter describes how the ZTX can be physically and logically inserted in an Arista network and provides reference configuration examples.

IP Communication requirements

As represented in the following logical diagram, there are two fundamental IP communication requirements for the ZTX Traffic Mapper:

a. The Traffic Mapper requires bidirectional IP communication with Arista **CloudVision** instance, using the **out-of-band** management interface, in order to
   i. export traffic metadata in IPFIX format
   ii. receive provisioning settings over HTTP
b. It also requires bidirectional IP communication over the **in-band** interfaces with the Arista switches that compose an **MSS Security Domain**, in order to
   i. receive monitored traffic from the switches over L2oGRE
   ii. maintain the healthiness of L2oGRE tunnels

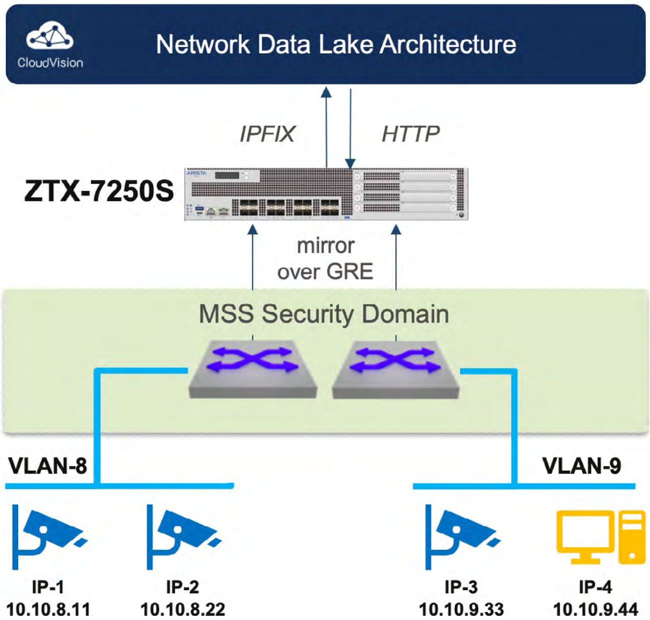


Fig.2 ZTX IP communication requirements.

Physical In-band Connectivity requirements

The ZTX Traffic Mapper capacity and port density are specific to each prodct.

The ZTX-7250S has a processing capacity of 80 Gbps and a physical connectivity capacity of 160 Gbps supplied by a range of sixteen 10 Gbps interfaces: Ethernet 1/1 - Ethernet 1/16.

The vZTX is available in either a 10G or 1G version, which have a respective processing capacity of either 10 Gpbs or 1 Gbps provided over two SR-IOV links of the same speed.

The processing power of the Traffic Mapper is used for extracting and exporting communication session metadata from mirrored traffic received by the switches that compose one - and one only - Security Domain. The traffic received by the ZTX consists of a copy (mirror) of the original layer-2 traffic packets that match one or more monitor rules, truncated to the first 256 or 192 bytes[1] and embedded into a L2oGRE envelope, which adds 42-46[2] bytes of overhead.

Physical connectivity options for the ZTX

Given its port density, there are two possible design options for the physical appliance: centralized or distributed, which are represented in the picture below.

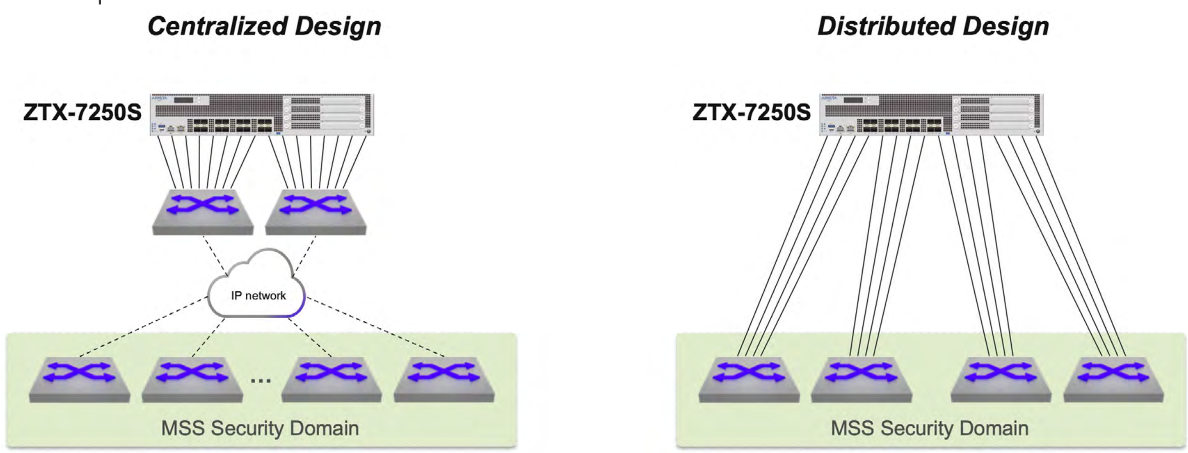


Fig.3: Topology Design options for ZTX: Centralized vs Distributed

[1] *This value is hardware platform dependent, not user configurable*
[2] *14-18 for Ethernet header, 20 for IP header, 4 for GRE header, 4 for optional GRE fields*

1. Centralized: the ZTX is placed within a service pod and its 16 interfaces are physically connected to a pair of switches that have IP connectivity to the Security Domain.

   This option is based on the best practice of using a dedicated self-contained unit in the network to provide all required network services with optimal scalability, efficiency and simplicity.

   With this approach, the planned network throughput of the service pod, needs to account for the theoretical inbound capacity of 80 Gbps of the ZTX, unless further rate limiters are applied in the data path from the Security Domain.

2. Distributed: the ZTX interfaces are evenly distributed to be directly adjacent to an even number of switches part of the Security Domain

   This option is recommended when the number of switches of the security domain is relatively small or when the interface speed of the ZTX does not match the one provided by existing switches in the service pod.

In both centralized and distributed options, the physical links of the ZTX that connect to the same physical device or, in case the peer devices use multi-chassis link aggregation, to the same device pair, can be grouped in a port channel. This choice may depend also on the selected routing design, which is discussed next.

Physical connectivity options for the vZTX

The recommended topology for vZTX consists in connecting each SR-IOV uplink to a different switch. The vZTX supports only routed ports and does not support link aggregation.

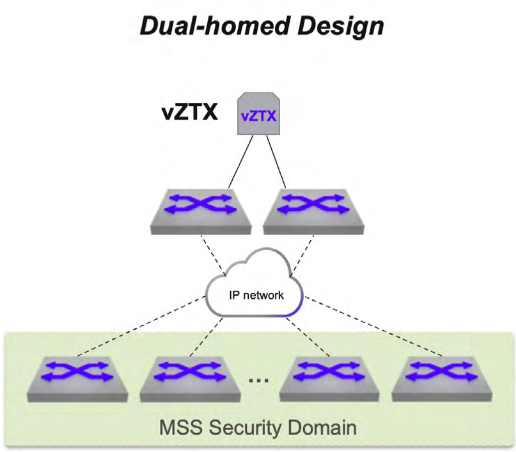


Fig.4: Topology Design options for vZTX: dual-homed

Logical In-band Network Requirements

To satisfy its in-band communication requirements, the Traffic Mapper must be provisioned with a distinct IP address, which needs to be reachable by the switches part of the Security Domain in order to create L2oGRE tunnels that use the Traffic Mapper address as destination. The IP address of the Traffic Mapper can be advertised to the adjacent switches via dynamic routing, or the adjacent switches can be configured with a specific static route that the adjacent switches can redistribute in their current routing protocol.

From an outbound routing direction perspective, the Traffic Mapper requires in its routing table either every loopback address of the switches of the Security Domain or an aggregate prefix that includes them. This information is needed for the sole purpose of a GRE tunnel health check, and can be also provided via dynamic or static routing.

IP Routing and Link Aggregation for the ZTX

In case the physical ZTX appliance is physically adjacent to a pair of switches that support MLAG, the choice of using dynamic vs. static routing influences the decision on how to bundle the ZTX interfaces into one or two port channels. The recommended design is as in the following table and diagrams:

ZTX adjacent to MLAG pair configured with:	Recommended number of port channels
Dynamic Routing	two (2)
Static Routing	one (1)

[3]The ZTX Traffic Mapper family supports the BGP protocol

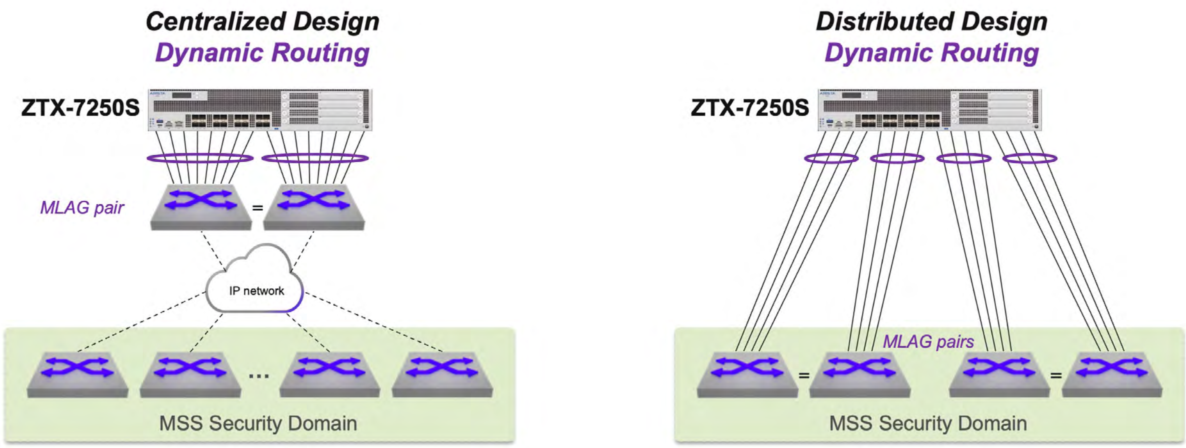


Fig.5: Recommended ZTX port aggregation design with MLAG peers in case of dynamic routing

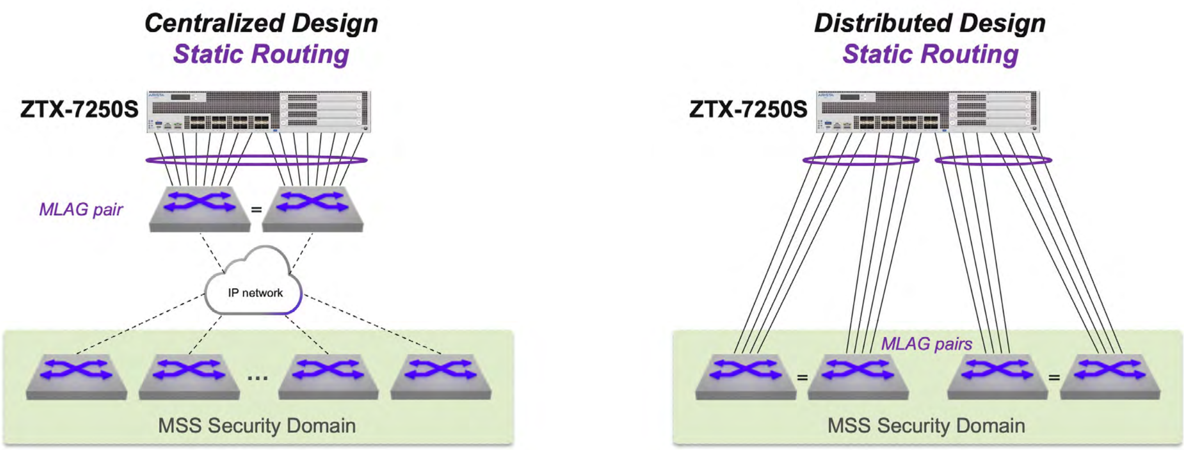


Fig.6: Recommended ZTX port aggregation design with MLAG peers in case of static routing

IP Routing for the vZTX

The vZTX supports routed port settings for its dual-homed links and can be deployed with either static or dynamic routing.

VRF and Security Zone Awareness

Monitoring rules are elements of MSS policies, configured on the Security Domain switches, which apply to a specific VRF, representing a determined security zone. On the ZTX, the VRF is identified via a GRE keyword field, present in the mirrored packet, and does not require to be declared in the device configuration.

L2GRE Tunnel Provisioning

The provisioning of L2oGRE tunnels on the ZTX and the Security Domain switches is automatic and triggered by creating or modifying monitoring rules and other MSS objects in CloudVision.

Traffic Mapping Service Settings

The traffic mapping service is pre-configured on the Traffic Mapper and in general does not require customization. Certain parameters - like the Active Timeout for IPFIX export - that require user input are provisioned in CloudVision upon associating a ZTX or vZTX device with a MSS Monitor Object, as later detailed in this guide.

The traffic mapping service classifies bidirectional TCP and UDP connections using the actual layer-4 destination port values, based on IANA definition of non-ephemeral port range: 0 to 1023 (well-known ports) and 1024 to 49151 (registered ports). Instead, connections using ephemeral ports, in the predefined range of 49152 to 65535, are reported with an aggregate value of 0.

The predefined ephemeral port range used by the Port Mapper can be customized with static CLI configuration, in case it is required to monitor certain applications that use ephemeral port numbers.

Configuration Examples

This chapter provides a few configuration examples that can be used to implement both out-of-band and in-band communication requirements for the Traffic Mapper.

Initial Configuration for vZTX

The Arista vZTX is offered in two versions respectively at 10 Gbps or 1 Gbps processing capacity and it is based on a generic vEOS virtual machine. The installation of vEOS is subject to meeting the hardware specification requirements for 10 Gbps and 1 Gbps version detailed in the ZTX datasheet. Installation is supported on the following servers with SR-IOV capable network adapters:

a. ESXi or KVM server

b. Arista vEOS Router Appliance

A post-installation step with required reboot is necessary to set up the correct Traffic Mapper profile on a generic vEOS virtual machine.

The initial vEOS Router profile is pre-configured and produces the following output:

```
# In this example, the VM has been allocated 4 CPU cores.
# On first-time installation
vZTX# bash cat /mnt/flash/veos-config
MODE=sfe
vZTX#
```

The following configuration steps change the profile to a Traffic Mapper, make the profile settings persistent and finally reboots the virtual machine to activate it:

```
vZTX# configure
vZTX(config)# firewall distributed instance
vZTX(config-firewall-distributed-instance)# no disabled
vZTX(config-firewall-distributed-instance)# end
vZTX# write
vZTX# reload
```

After reboot, the new profile settings can be verified as following:

```
vZTX# bash cat /mnt/flash/veos-config
MODE=sfe
platformRuby=True
maxDatapathCores=2
vZTX#
```

Note that the value of the parameter maxDatapathCores is automatically configured based on the number of CPU cores allocated for the virtual machine.

Customizing Traffic Mapping Service Settings

This configuration example documents how it is possible to modify the predefined ephemeral port range on a ZTX or vZTX device, in order to record destination port numbers with high values in the TCP or UDP connection records, which otherwise are recorded with an aggregated value of 0.

The example assumes an HDFS application implemented with port numbers that IANA classifies as ephemeral, like: 50010, 50020, 50070, 50090, 50470, 50475. By default, connections of this application are reported by the Traffic Mapper with a null destination port number, instead of their actual values above. To change this behavior, it is necessary to reduce the set of ephemeral port numbers from the default range of 49152-65535 to a custom range of 50476-65535.

This operation is achieved with a CLI configuration that, in earlier software versions, is not activated on the ZTX/vZTX:

```
firewall distributed instance
   ephemeral-port destination start 50476
!
```

Out-of-band Configuration Pre-requisites

As a prerequisite, the Traffic Mapper requires an IP address assigned to its management interface and an active Streaming Agent (TerminAttr) instance, in order to communicate with CloudVision. Refer to CloudVision documentation to understand the different options to onboard an Arista device in CloudVision.

This example assumes that:

- The CloudVision cluster uses the following IP addresses: 172.28.137.75, 172.28.130.47, 172.28.133.90
- The ZTX device is provisioned with at least one valid NTP server and with the proper clock time-zone, for example:

```
ntp server my-ntp-server.mydomain.mycompany.com
!
clock timezone US/Pacific
!
```

- The Traffic Mapper device is provisioned with a management address of 172.28.137.229/20 and a default gateway in the default VRF:

```
interface Management1/1
ip address 172.28.137.229/20
!
ip route 0.0.0.0/0 172.28.128.1
```

The resulting Streaming Agent configuration after onboarding the Traffic Mapper device in CloudVision is as following:

Note that the existing code above reflects the IP addresses of CloudVision and the VRF value (default) of the management interface.

```
daemon TerminAttr
   exec /usr/bin/TerminAttr
-smashexcludes=ale,flexCounter,hardware,kni,pulse,strata
-cvaddr=172.28.137.75:9910,172.28.130.47:9910,172.28.133.90:9910
-cvauth=token,/tmp/token -cvvrf=default -taillogs
   no shutdown
!
```

ZTX In-band Configuration Example with MLAG Peering and Static Routing

This example is based on the following topology diagram, where the ZTX is physically adjacent to a pair of Arista switches configured as MLAG peers, and a single port channel group is established between them.

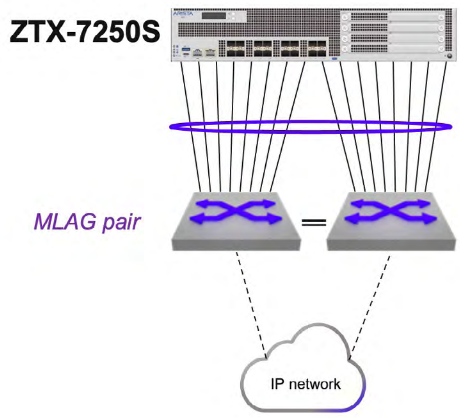


Fig.7: Topology example of MLAG peering and static routing

These are in summary the configuration steps for this example:

1. A single port channel is provisioned on both the ZTX and MLAG pair.
2. The ZTX is configured with a unique IP address in a specific subnet that is assigned to an SVI.
3. The VLAN used by this SVI is configured on the port channel on both the ZTX and the MLAG pair.
4. The same IP subnet is assigned to the corresponding SVI on the MLAG pair.
5. The ZTX is configured with a static route in order to have reachability to the switches in the Security Domain.
6. The MLAG pair communicates with the rest of the IP network with a dynamic protocol of choice and advertises the local subnet of the SVI to provide reachability to the ZTX IP address.
7. The ARP timeout of the ZTX is tuned to achieve peer adjacency persistence

Following the configuration step details:

8. A single port channel is provisioned on both the ZTX and MLAG pair.

   On ZTX:

```
interface Port-Channel16
!
interface Ethernet1/1 - Ethernet1/16
   channel-group 16 mode active
!
```

   On MLAG left and right switches:

```
interface Port-Channel8
   mlag 8
!
interface Ethernet11/1 - 4
   speed forced 10000full
   channel-group 8 mode active
!
interface Ethernet13/1 - 4
   speed forced 10000full
   channel-group 8 mode active
!
```

9. The ZTX is configured with a unique IP address in a specific subnet that is assigned to an SVI.

```
vlan 1016
!
interface vlan1016
   ip address 10.10.16.4/29
!
```

10. The VLAN used by this SVI is configured on the port channel on both the ZTX and the MLAG pair.

    On the ZTX:

```
interface Port-Channel16
   switchport access vlan 1016
!
```

    On the MLAG switch pair:

```
vlan 1016
!
interface Port-Channel8
   switchport access vlan 1016
!
```

11. The same IP subnet is assigned to the corresponding SVI on the MLAG pair.

    On both left and right switch:

```
interface vlan1016
   ip virtual address 10.10.16.1/29
!
```

12. The ZTX is configured with a static route in order to have reachability to the switches in the Security Domain.

    Assuming these switches use addresses taken from a 10.10.0.0/19 aggregate subnet:

```
ip routing
!
ip route 10.0.0.0/19 10.10.16.1
```

13. The MLAG pair communicates with the rest of the IP network with a dynamic protocol of choice and advertises the locally connected subnet of the SVI to provide reachability to the ZTX IP address.

    For example, using OSPF:

```
router ospf 10
   redistribute connected
!
```

14. The ARP timeout of the ZTX is tuned to achieve peer adjacency persistence
    This step is recommended with static routing and ensures that the layer-2 adjacency does not expire in case monitoring is inactive and peer links are idle.

```
arp aging timeout default 180
```

ZTX In-band Configuration Example with Dynamic Routing

This example is based on the following topology diagram, where the ZTX is physically adjacent to two or more Arista switches, and one channel group per switch is established between them. In case the peering switches are two, they can optionally form an MLAG pair.

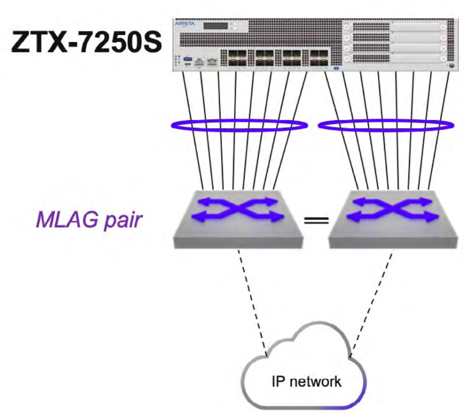


Fig.8: Topology example of layer-3 peering and dynamic routin

These are in summary the configuration steps for this example:

1. A single routed port channel is provisioned on the ZTX and each peering switch, and configured with a point-to-point subnet
2. The ZTX is configured with a unique host IP address that is assigned to a loopback interface.
3. The ZTX is configured with a dynamic routing protocol and peering with the adjacent switches, in order to have mutual reachability between its loopback address and those assigned to the switches in the Security Domain.

Following the configuration step details:

4. A single routed port channel is provisioned on the ZTX and each peering switch, and configured with a point-to-point subnet

```
interface Port-Channel8
   no switchport
   ip address 192.168.100.101/31
!
interface Ethernet1/1 - Ethernet1/8
   channel-group 8 mode active
!
interface Port-Channel16
   no switchport
   ip address 192.168.100.103/31
!
interface Ethernet1/9 - Ethernet1/16
   channel-group 16 mode active
!
```

On left peering switch:

```
interface Port-Channel8
   no switchport
   ip address 192.168.100.100/31
!
interface Ethernet11/1 - 4
   speed forced 10000full
   channel-group 8 mode active
!
interface Ethernet13/1 - 4
   speed forced 10000full
   channel-group 8 mode active
!
```

On right peering switch:

```
interface Port-Channel16
   no switchport
   ip address 192.168.100.102/31
!
interface Ethernet11/1 - 4
   speed forced 10000full
   channel-group 16 mode active
!
interface Ethernet13/1 - 4
   speed forced 10000full
   channel-group 16 mode active
!
```

5. The ZTX is configured with a unique host IP address that is assigned to a loopback interface.

```
interface Loopback0
   description router-id
   ip address 10.135.2.16/32
!
```

6. The ZTX is configured with a dynamic routing protocol, in this example BGP, and peering with the adjacent switches, in order to have mutual reachability between its loopback address and those assigned to the switches in the Security Domain.

   On ZTX:

```
router bgp 64516
   router-id 10.135.2.16
   distance bgp 20 200 200
   maximum-paths 2
   neighbor UNDERLAY peer group
   neighbor UNDERLAY maximum-routes 120
   neighbor 192.168.100.100 peer group UNDERLAY
   neighbor 192.168.100.100 remote-as 64504
   neighbor 192.168.100.100 description SwitchLeft
   neighbor 192.168.100.102 peer group UNDERLAY
   neighbor 192.168.100.102 remote-as 64504
   neighbor 192.168.100.102 description SwitchRight
   redistribute connected
   !
   address-family ipv4
      neighbor UNDERLAY activate
!
```

On left peering switch:

```
router bgp 64504
   network 10.135.2.0/24
   neighbor ZTX peer group
   neighbor ZTX route-map LOOPBACKS out
   neighbor 192.168.100.101 peer group ZTX
   neighbor 192.168.100.101 remote-as 64516
   neighbor 192.168.100.101 description ZTX-1
   !
   address-family ipv4
      neighbor ZTX activate
!
route-map LOOPBACKS permit 10
   match ip address prefix-list LOOPBACKS
!
ip prefix-list LOOPBACKS seq 5 permit 10.135.2.0/24
!
```

On right peering switch

```
router bgp 64504
   network 10.135.2.0/24
   neighbor ZTX peer group
   neighbor ZTX peer group
   neighbor ZTX route-map LOOPBACKS out
   neighbor 192.168.100.103 peer group ZTX
   neighbor 192.168.100.103 remote-as 64516
   neighbor 192.168.100.103 description ZTX-1
   !
   address-family ipv4
      neighbor ZTX activate
!
route-map LOOPBACKS permit 10
   match ip address prefix-list LOOPBACKS
!
ip prefix-list LOOPBACKS seq 5 permit 10.135.2.0/24
!
```

vZTX In-band Configuration Examples with Static and Dynamic Routing

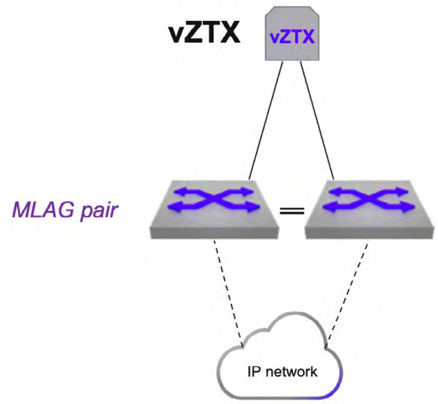


Fig.9: Topology example of layer-3 peering and static or dynamic routing

Following the configuration step details:

1. A single routed interface is provisioned on the vZTX and each peering switch, and configured with a unique subnet, for example using a point-to-point subnet:

```
interface Ethernet1
   no switchport
   ip address 192.168.100.101/31
!
interface Ethernet2
   no switchport
   ip address 192.168.100.103/31
!
```

On left peering switch:

```
interface Ethernet11/1
   speed forced 10000full
   no switchport
   ip address 192.168.100.100/31
!
```

On right peering switch:

```
interface Ethernet11/1
   speed forced 10000full
   no switchport
   ip address 192.168.100.102/31
!
```

2. The vZTX is configured with a unique host IP address that is assigned to a loopback interface.

```
interface Loopback0
   description router-id
   ip address 10.135.2.16/32
!
```

3. A The vZTX is configured with two static routes in order to have reachability to the switches in the Security Domain.

   Assuming these switches use addresses taken from a 10.10.0.0/19 aggregate subnet:

```
ip routing
!
ip route 10.0.0.0/19 192.168.100.100
ip route 10.0.0.0/19 192.168.100.102
```

4. A The peer switch pair communicates with the rest of the IP network with a dynamic protocol of choice and advertises local static routes to provide reachability to the vZTX IP address.

   For example, using OSPF:

```
ip route 10.135.2.16/32 192.168.100.101
ip route 10.135.2.16/32 192.168.100.103
router ospf 10
   redistribute static
!
```

5. A The ARP timeout of the vZTX and the peering switches is tuned to achieve peer adjacency persistence.

   This step is recommended with static routing and ensures that the layer-2 adjacency does not expire in case monitoring is inactive and peer links are idle.

   On vZTX:

```
arp aging timeout default 180
```

   On peering switches:

```
arp aging timeout default 180
```

3. B As an alternative to previous points 3.A - 5.A, the vZTX can be configured with a dynamic routing protocol, in this example BGP, and peering with the adjacent switches, in order to have mutual reachability between its loopback address and those assigned to the switches in the Security Domain.

On vZTX:

```
router bgp 64516
   router-id 10.135.2.16
   distance bgp 20 200 200
   maximum-paths 2
   neighbor UNDERLAY peer group
   neighbor UNDERLAY maximum-routes 120
   neighbor 192.168.100.100 peer group UNDERLAY
   neighbor 192.168.100.100 remote-as 64504
   neighbor 192.168.100.100 description SwitchLeft
   neighbor 192.168.100.102 peer group UNDERLAY
   neighbor 192.168.100.102 remote-as 64504
   neighbor 192.168.100.102 description SwitchRight
   redistribute connected
   !
   address-family ipv4
      neighbor UNDERLAY activate
!
```

On left peering switch:

```
router bgp 64504
   network 10.135.2.0/24
   neighbor ZTX peer group
   neighbor ZTX route-map LOOPBACKS out
   neighbor 192.168.100.101 peer group ZTX
   neighbor 192.168.100.101 remote-as 64516
   neighbor 192.168.100.101 description ZTX-1
   !
   address-family ipv4
      neighbor ZTX activate
!
route-map LOOPBACKS permit 10
   match ip address prefix-list LOOPBACKS
!
ip prefix-list LOOPBACKS seq 5 permit 10.135.2.0/24
!
```

On right peering switch:

```
router bgp 64504
   network 10.135.2.0/24
   neighbor ZTX peer group
   neighbor ZTX peer group
   neighbor ZTX route-map LOOPBACKS out
   neighbor 192.168.100.103 peer group ZTX
   neighbor 192.168.100.103 remote-as 64516
   neighbor 192.168.100.103 description ZTX-1
   !
   address-family ipv4
      neighbor ZTX activate
!
route-map LOOPBACKS permit 10
   match ip address prefix-list LOOPBACKS
!
ip prefix-list LOOPBACKS seq 5 permit 10.135.2.0/24
!
```

Managing the Traffic Mapper with CloudVision

After the ZTX or vZTX device has been onboarded to CloudVision and the in-band communication with the Security Domain is complete, the next step is to associate it with a MSS Monitor Object in CloudVision, so it can be referenced by one or more policy rules.

An MSS Monitor Object is a structure that defines how a Traffic Mapper device can communicate with a Security Domain.

The definition of a Monitor Object is possible from the MSS Service studio, which, once enabled in General Settings, is available under Network Services in the Studios pane, as shown in the screenshot below.

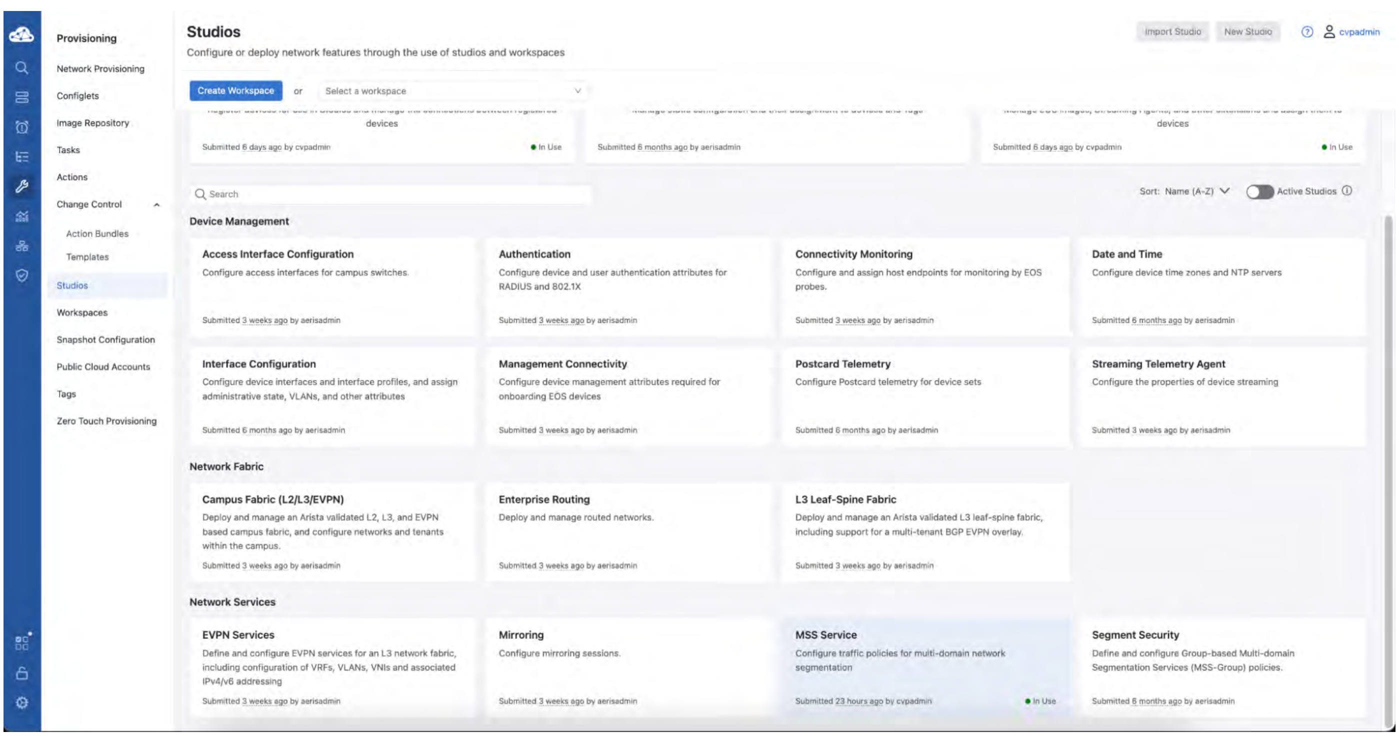


Fig.10: CloudVision: MSS Service studio selection

As for any other studio, before making any edit to the MSS objects, a change-control workspace needs to be created, as shown in the following screenshot.

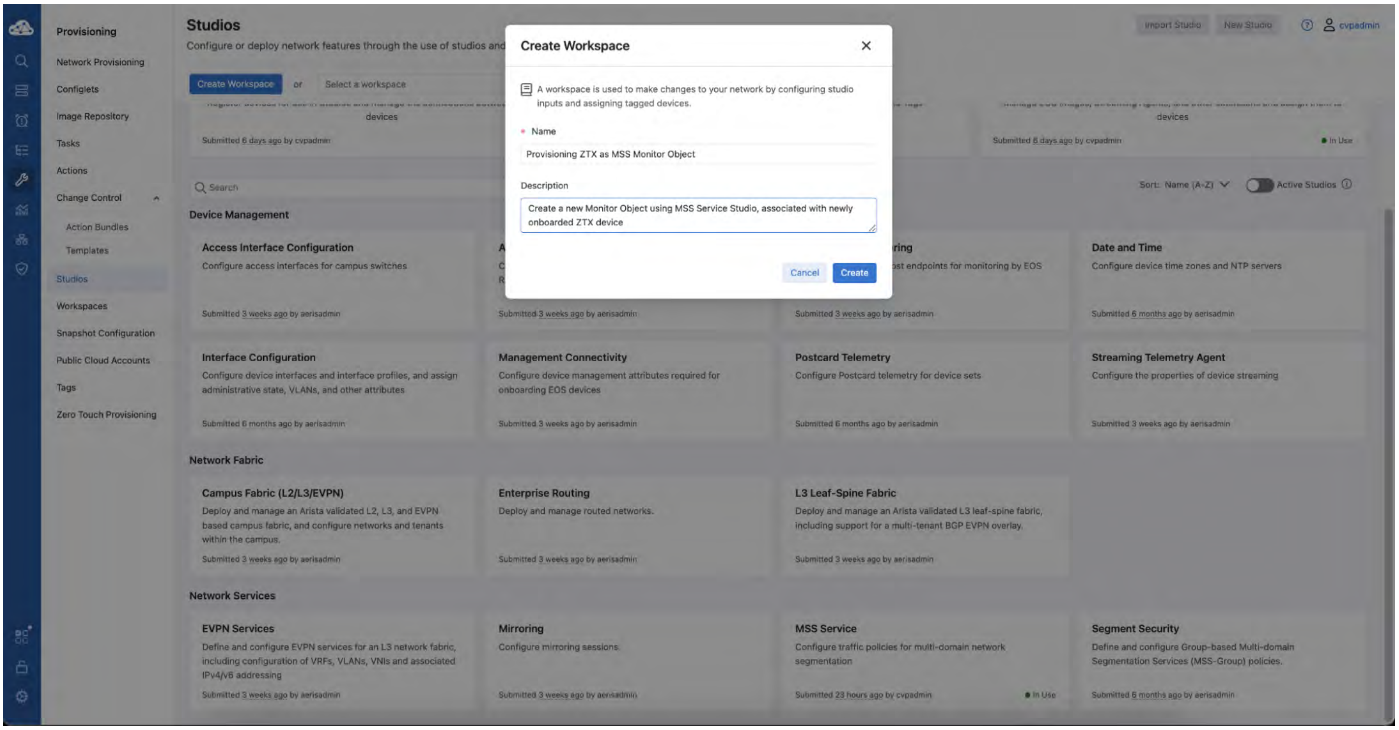


Fig.11: CloudVision: change-control workspace creation

The studio form presents most of the MSS objects structured in a multi-level tabular format. Monitor Objects are listed in a dedicated table in the bottom portion of the studio. A new object can be defined using the "Add Monitor Object" button, as shown in the screenshot below:

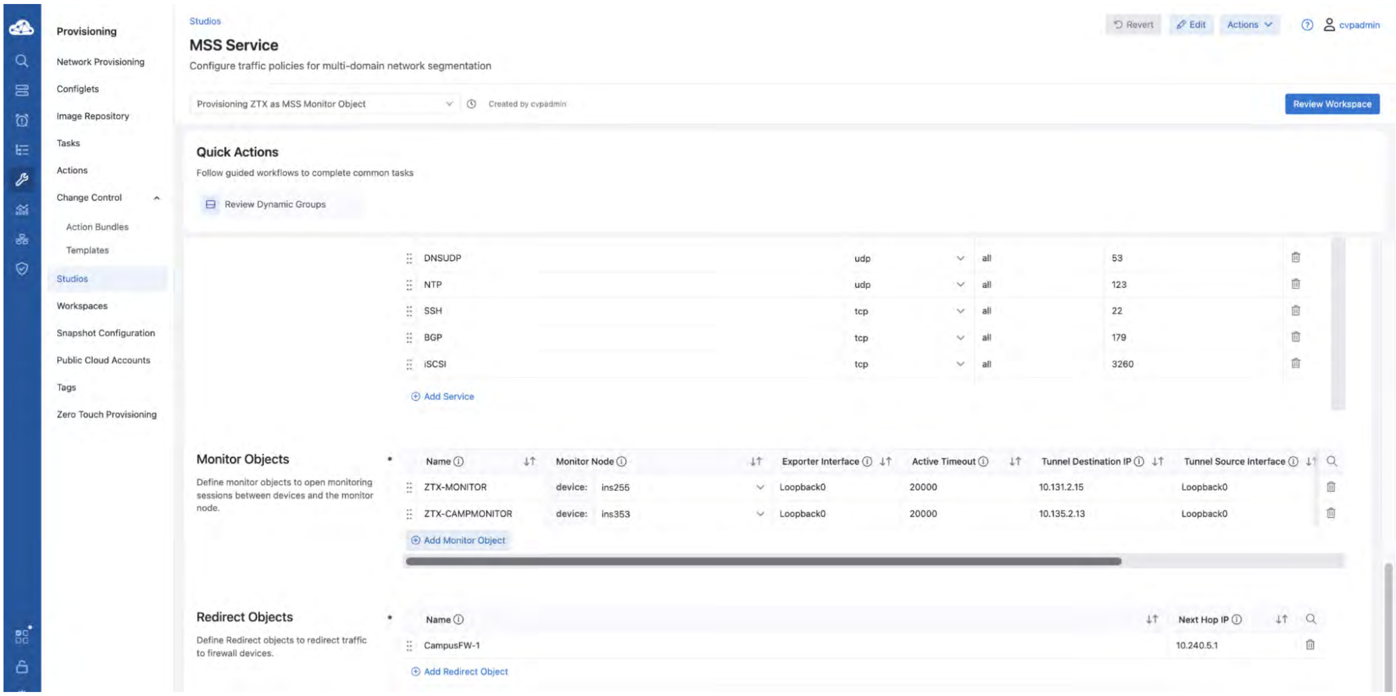


Fig.12: CloudVision: Monitor Object table in MSS Service studio

The definition of a Monitor Object, requires entering values for the following mandatory parameters:

Parameter	Description	Recommended Value
Name	Unique string identifying the Monitor Object that can be referenced by a policy rule	
Monitor Node	Associated ZTX device among those present in the device inventory	
Exporter Interface	Interface name on the ZTX that is used as IPFIX exporter and L2GRE tunnel termination	
Active Timeout	Active timeout period in ms for exporting IPFIX reports	long-term setting: 30000 – 300000 ms temporarily for initial deployment: 3000 - 30000 ms
Tunnel Destination IP	IP address of the ZTX used as L2GRE tunnel destination on switches part of the Security Domain	
Tunnel Source Interface	Interface name on the Security Domain switches used as L2GRE tunnel source. All switches use consistently the same interface name.	
Truncation	Boolean field, indicating if mirrored traffic is truncated or not	Yes
Rate Limit	Rate limiter expressed in Mbps applied on Security Domain switches to mirrored traffic per VRF sent to the ZTX	10,000

Once a new Monitor Object entry has been populated with all required values, it is possible to select it inside the field "Monitor Name" in multiple policy rules part of the same policy.

The same Monitor Object can be concurrently referred to by multiple policies, while a policy (associated to a security zone) can only use one Monitor Object.

First, it is necessary to navigate in the studio form to the "Policies" table, and from there, by clicking on the desired policy entry in the "Rules" column, it is possible to view and edit the corresponding policy rules. The following two screenshots are provided as a reference.

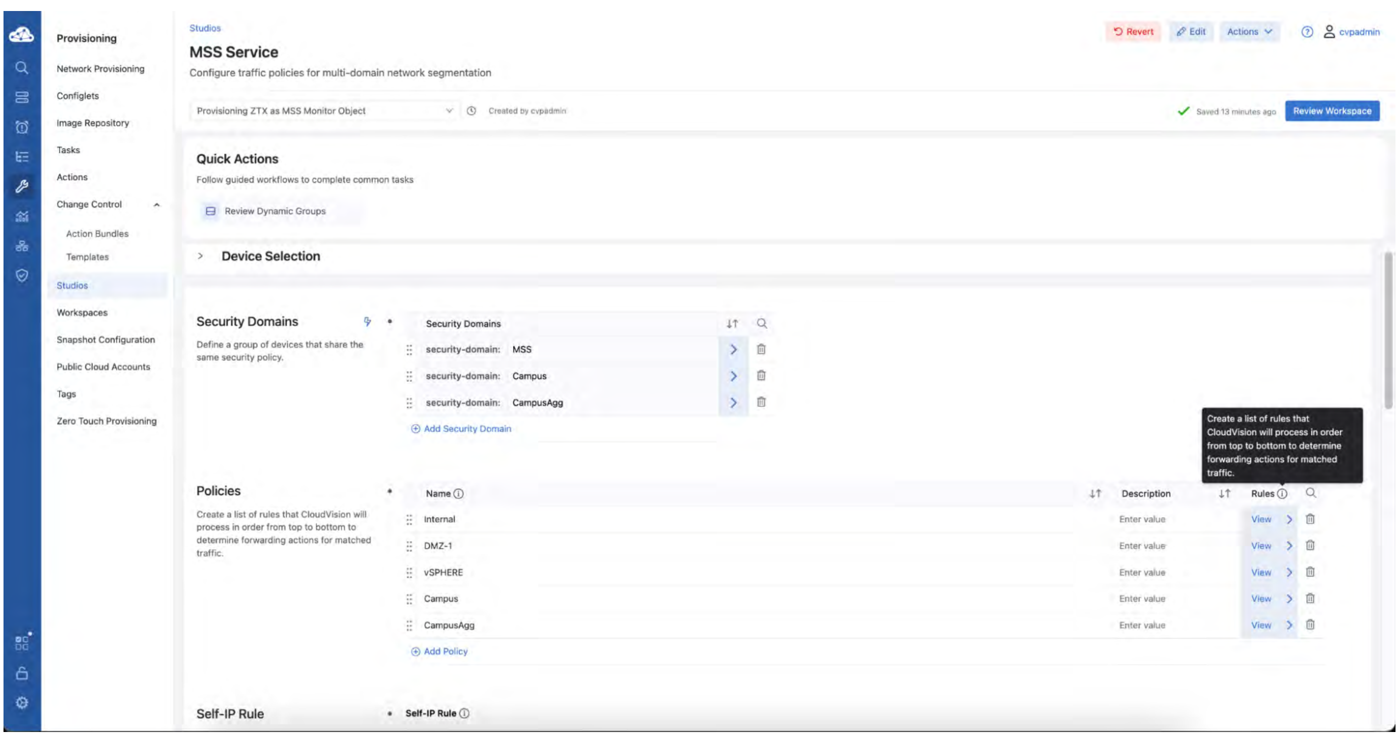


Fig.13: CloudVision: Policies table in MSS Service studio

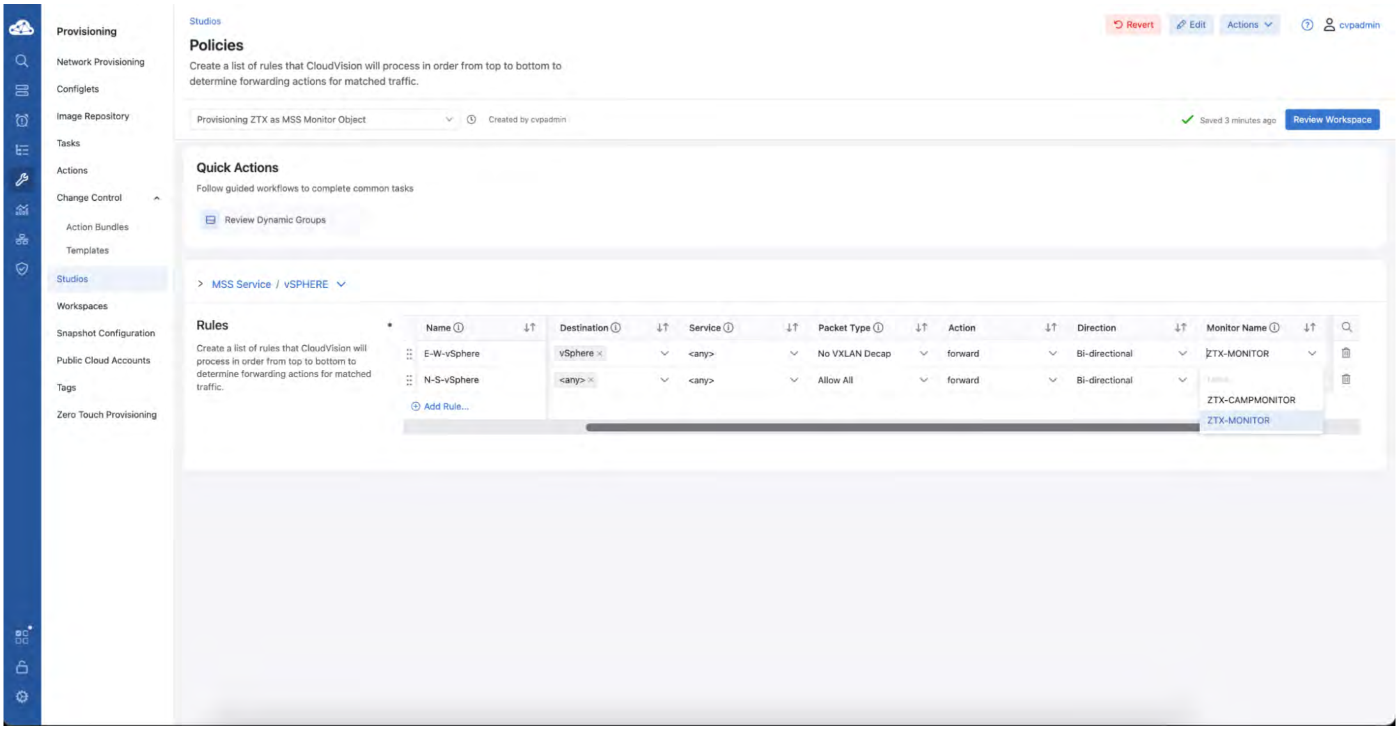


Fig.14: CloudVision: Rules table in MSS Service studio

Once a new Monitor Object entry has been created, it is necessary to validate its parameters by clicking on the Autofill button located on the top left portion of the studio form, as shown below.

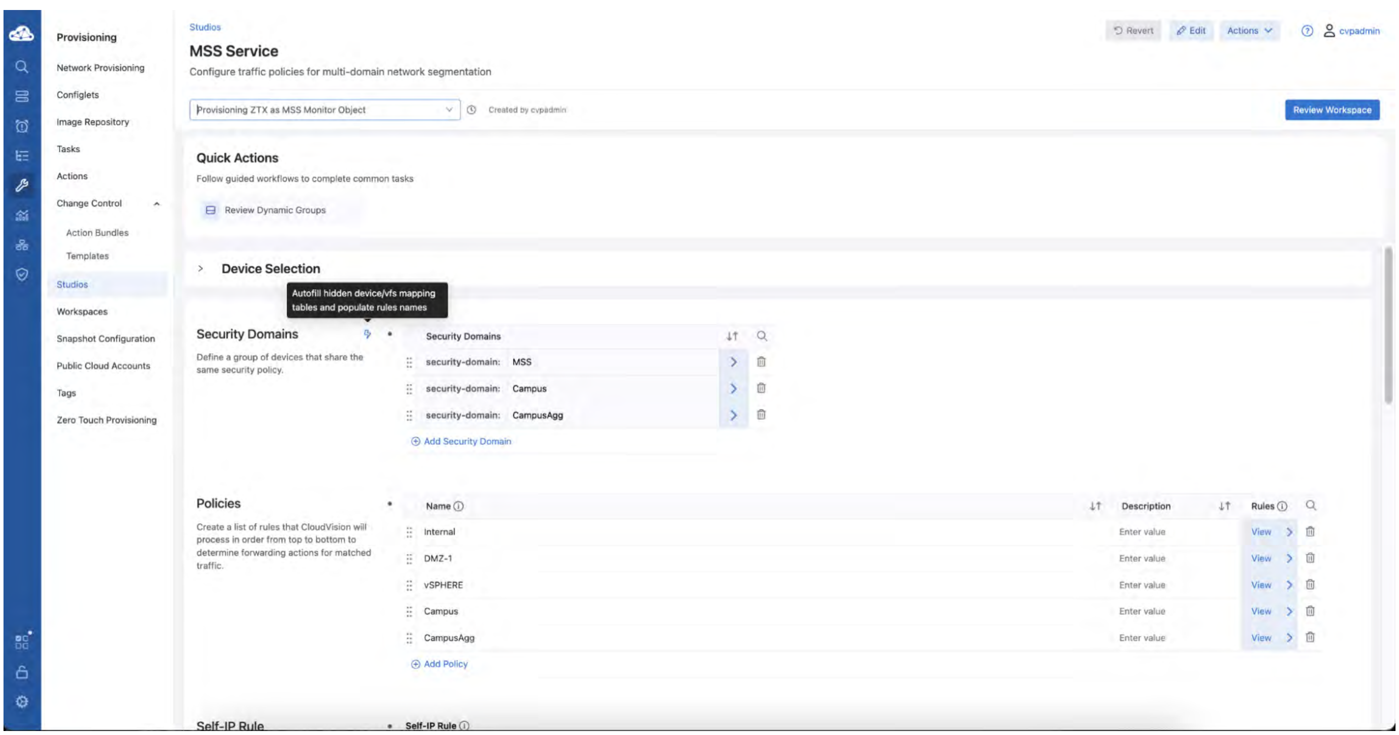


Fig.15: CloudVision: auto-fill button in MSS Service studio

If no errors are reported, the change-control workspace can be reviewed, using the top right "Review Workspace" button, and subsequently executed, following the same workflow used by other studios.

Monitor Object: Configuration Examples

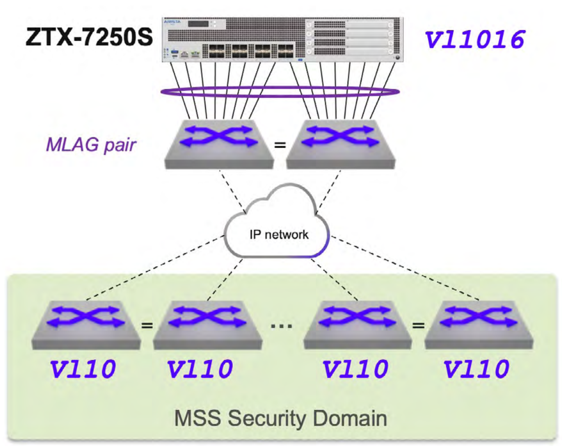
The following chapters include some examples for two Monitor Object parameters that are used to automatically provision the L2GRE transport and that have a dependency on the network topology and design: these are the Exporter Interface, which is a Traffic Mapper attribute and the Tunnel Source Interface, which is a common property of all Security Domain switches.

Using the following network diagrams as reference, the examples apply to three slightly different network topologies, where the IP addresses for in-band communication are assigned to different interfaces on the Traffic Mapper and on the switches part of the Security Domain.

Referencing the topology examples below, the following entries are valid entries of values assigned to the Exporter Interface and Tunnel Source Interface of an MSS Monitor Object:

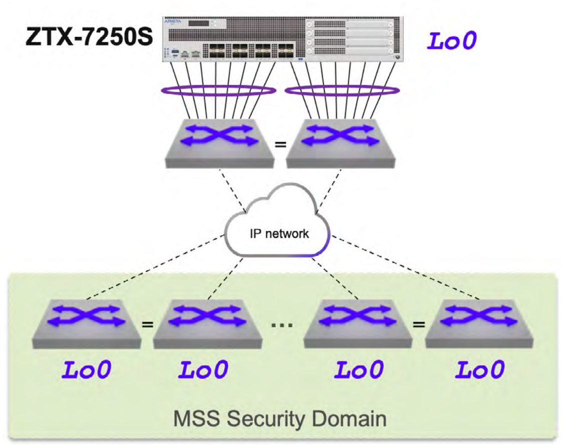
Topology	Monitor Object	Exporter Interface	Tunnel Source Interface
ZTX Example-1	Monitor-Example-A	Vlan1016	Vlan10
ZTX Example-2	Monitor-Example-B	Loopback0	Loopback0
vZTX Example-3	Monitor-Example-C	Loopback0	Loopback0

ZTX Topology Example #1



Interface	Description
Vlan 1016	Unique IP address assigned to the ZTX physical appliance. VLAN 1016 is used for layer-2 peering with adjacent switches
Vlan 10	Unique IP address assigned to each switch of the Security Domain. VLAN 10 is used by each switch for peering with upstream network

ZTX Topology Example #2



Interface	Description
Loopback0	Unique IP address assigned to the physical ZTX appliance
Loopback0	Unique IP address assigned to each switch of the Security Domain

Fig.17: ZTX Exporter and Tunnel Source Interface examples using loopback interfaces

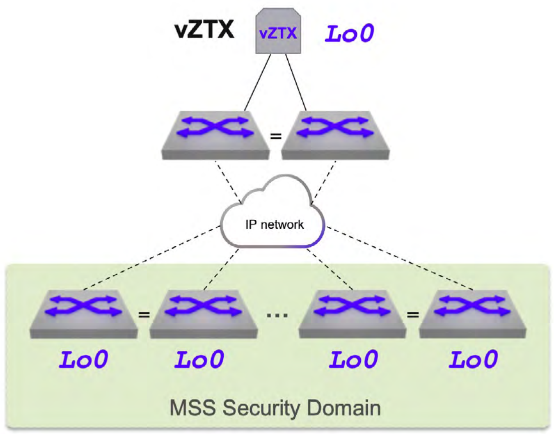
vZTX Topology Example #3	Interface	Description
	Loopback0	Unique IP address assigned to the vZTX appliance
	Loopback0	Unique IP address assigned to each switch of the Security Domain

Fig.18: vZTX Exporter and Tunnel Source Interface examples using loopback interfaces

References

NIST Zero Trust Architecture

https://www.nist.gov/publications/zero-trust-architecture

Arista MSS Technical Whitepaper

https://www.arista.com/assets/data/pdf/Whitepapers/MSS-Segmentation-Technical-WP.pdf

Arista MSS Datasheet

https://www.arista.com/assets/data/pdf/Datasheets/Multi-Domain-Segmentation-Services-for-Zero-Trust-Networking.pdf

Arista ZTX Traffic Mapper Datasheet

https://www.arista.com/assets/data/pdf/Datasheets/ZTX-7250S-MSS-Traffic-Mapper.pdf

Arista CloudEOS and vEOS Router Appliance Guide

https://www.arista.com/assets/data/pdf/qsg/qsg-books/QS_RA_200_vEOS.pdf

Arista CloudEOS and vEOS Router Configuration Guide

https://www.arista.com/assets/data/pdf/user-manual/um-books/CloudEOS_vEOS_Router_Config_Guide.pdf

Arista CloudVision Help Center

https://www.arista.io/help/articles/b3ZlcnZpZXcubXNzLm92ZXJ2aWV3

IEEE 802.1Q - Standard for Local and Metropolitan Area Networks - Bridges and Bridged Networks

https://ieeexplore.ieee.org/document/10004498

Santa Clara—Corporate Headquarters
5453 Great America Parkway,
Santa Clara, CA 95054

Phone: +1-408-547-5500
Fax: +1-408-538-8920
Email: info@arista.com

Ireland—International Headquarters
3130 Atlantic Avenue
Westpark Business Campus
Shannon, Co. Clare
Ireland

Vancouver—R&D Office
9200 Glenlyon Pkwy, Unit 300
Burnaby, British Columbia
Canada V5J 5J8

San Francisco—R&D and Sales Office 1390
Market Street, Suite 800
San Francisco, CA 94102

India—R&D Office
Global Tech Park, Tower A, 11th Floor
Marathahalli Outer Ring Road
Devarabeesanahalli Village, Varthur Hobli
Bangalore, India 560103

Singapore—APAC Administrative Office
9 Temasek Boulevard
#29-01, Suntec Tower Two
Singapore 038989

Nashua—R&D Office
10 Tara Boulevard
Nashua, NH 03062