Automating Micro-Segmentation and Deploying Layer 4-7 Services in VXLAN EVPN Fabrics using Group Policy Option (GPO) and Nexus Dashboard

Alessandro De Prato
Technical Marketing Engineer

cisco Live !

Webex App

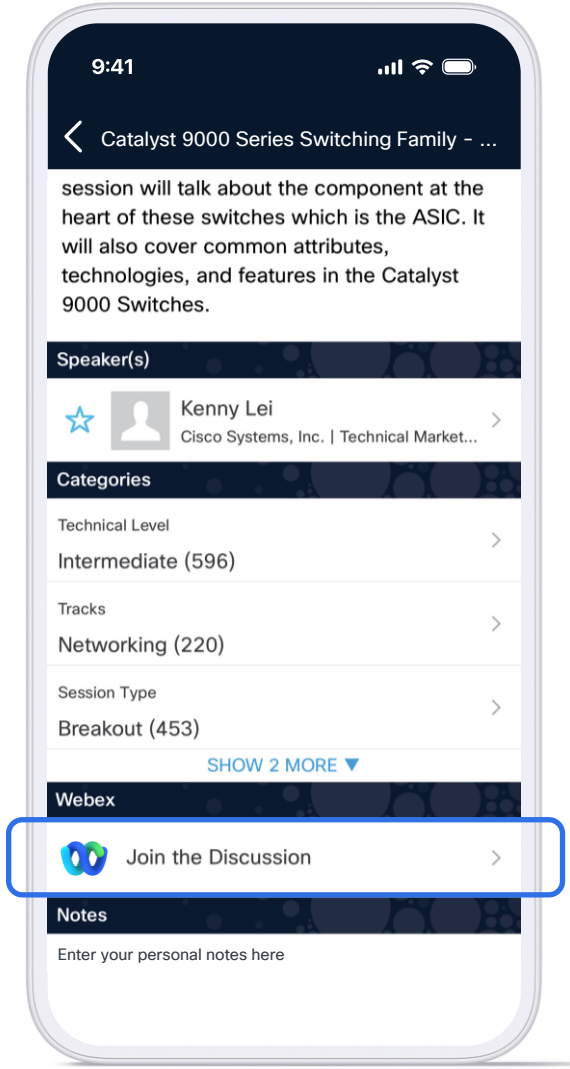
Questions?

Use Webex App to chat with the speaker after the session

How

1. Find this session in the Cisco Events App
2. Click “Join the Discussion”
3. Install the Webex App or go directly to the Webex space
4. Enter messages/questions in the Webex space

Webex spaces will be moderated by the speaker until February 27, 2026.



Agenda

01 Introduction

02 Group Policy Option Review

03 Group Policy Option Use Cases

04 GPO Based Service Redirection

Introduction

Group Policy Option

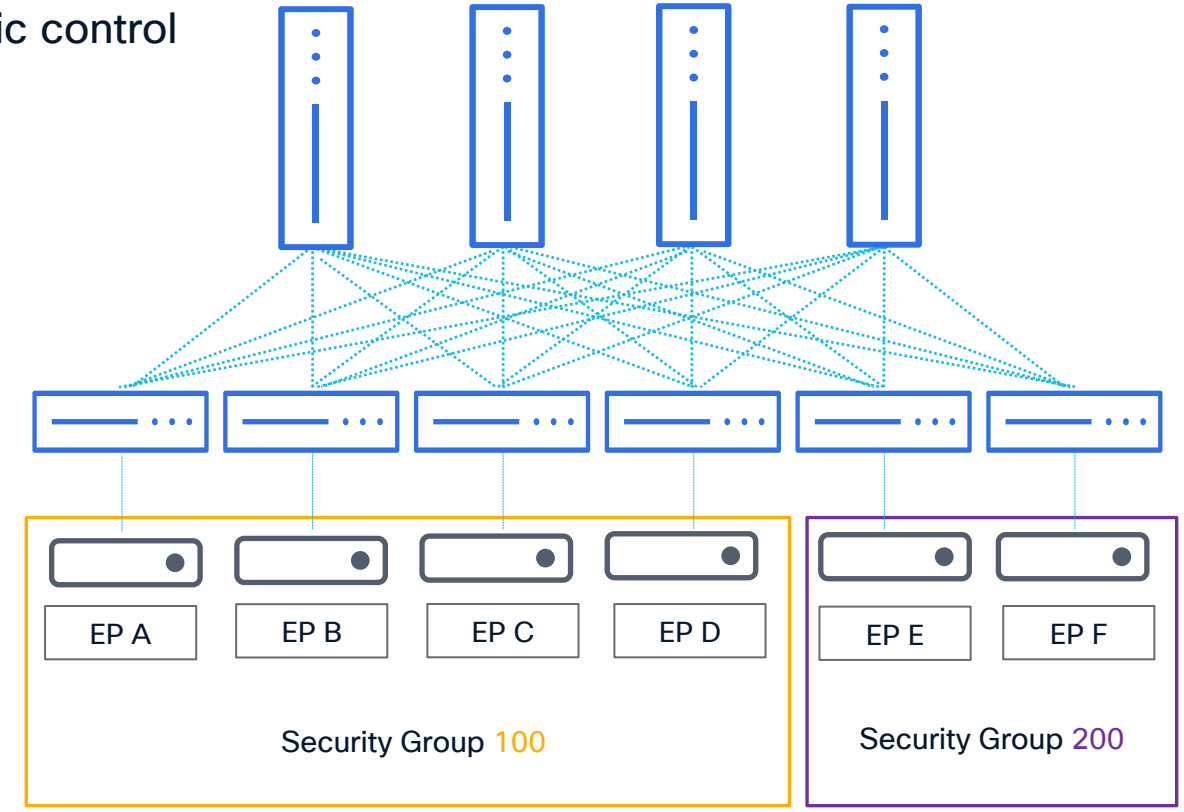
Enhancing Data Center Segmentation with Simplicity and Granularity

- Data Center security is important
- Threats are evolving, increasing and becoming more complex
- Enforce organization’s security standards by permitting only pre-approved traffic across and within every network segment
- Traffic enforcement needs to optimized. Design and configurations must be streamlined
- Newer capabilities have been introduced in recent NX-OS to expand the existing feature-set
  - Group Policy Option
  - Service Redirection based on GPO

Group Policy Option

Enhancing Data Center Segmentation with Simplicity and Granularity

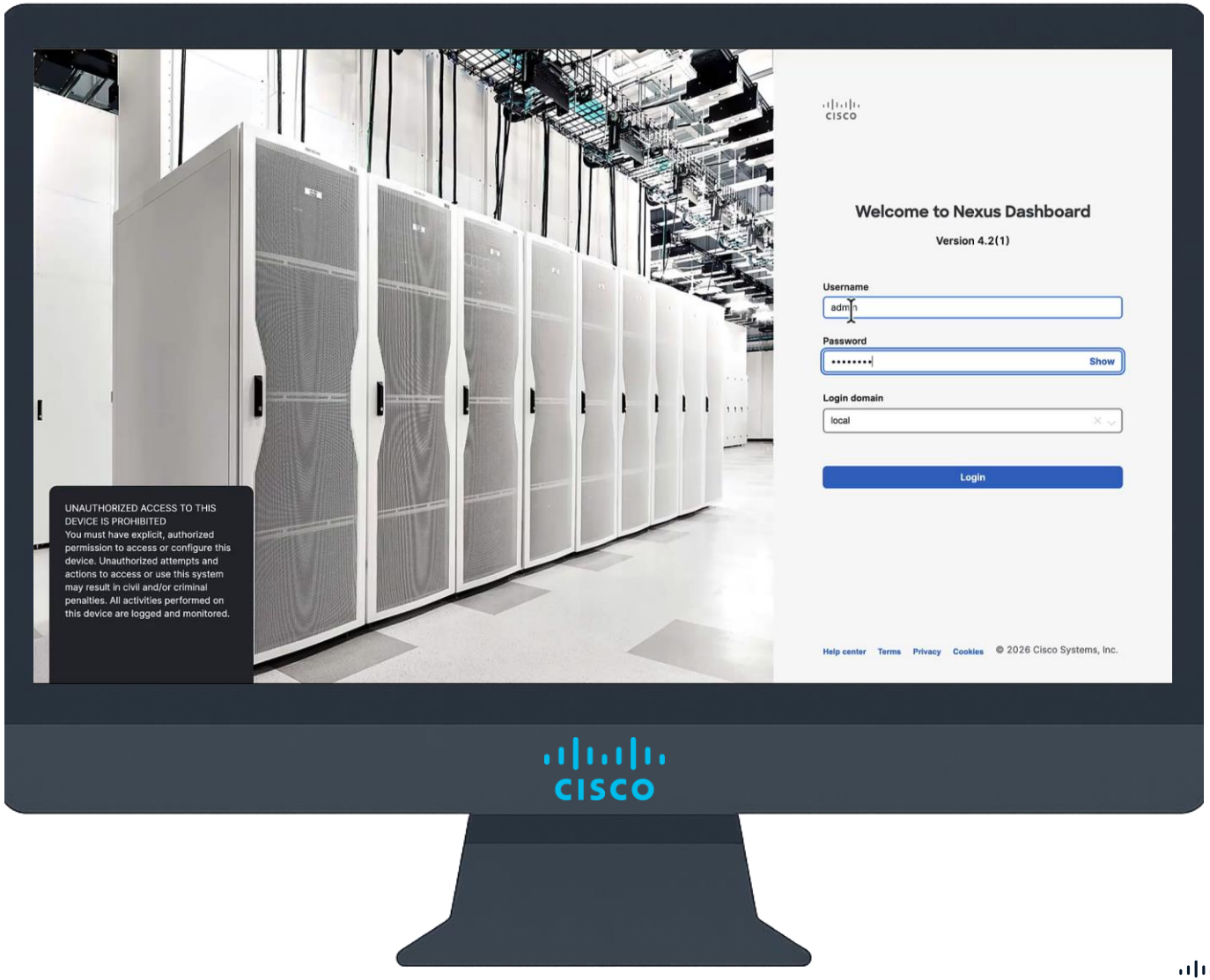
- GPO Standard
  - Extension to VXLAN and EVPN that provide additional traffic control
- Grouping
  - Resources in a group inherit the same policies
- Classification
  - Classify endpoints into security-groups
    - Based on IPs, MACs, VLANs and Ports
- Enforcement for inter-group traffic
  - Action: Permit, Deny, Redirect
  - Supports micro-segmentation
- Easily **automated** via Nexus Dashboard
- Easily **monitored** via Nexus Dashboard



Group Policy Option

Controller Requirements

- Nexus Dashboard is highly recommended but optional
- Support for GPO added in ND 3.2
- Seamless workflows to help administrators define the Data Center security posture
- Single-Site and Multi-Site supported
- Requires “cli” overlay mode, “config-profiles” are not supported
  - Migration soon available! (**ND 4.2)**
- Day-2 tools to monitor status, forwarding and counters

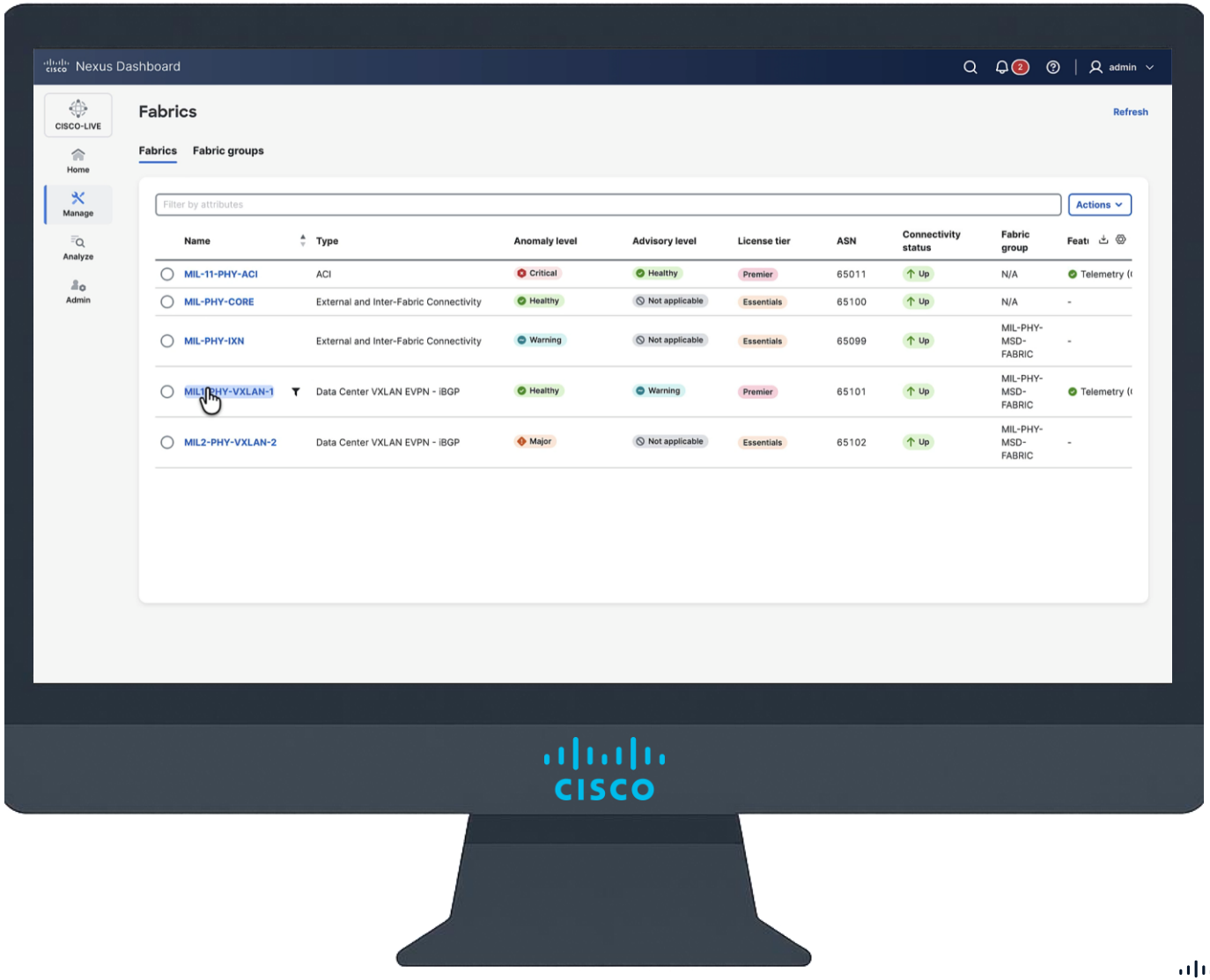


Note: Demos and Screenshots based on ND 4.2 beta

Group Policy Option

Controller Requirements

- Nexus Dashboard is highly recommended but optional
- Support for GPO added in ND 3.2
- Seamless workflows to help administrators define the Data Center security posture
- Single-Site and Multi-Site supported
- Requires “cli” overlay mode, “config-profiles” are not supported
    - Migration soon available! (**ND 4.2)**
- Day-2 tools to monitor status, forwarding and counters



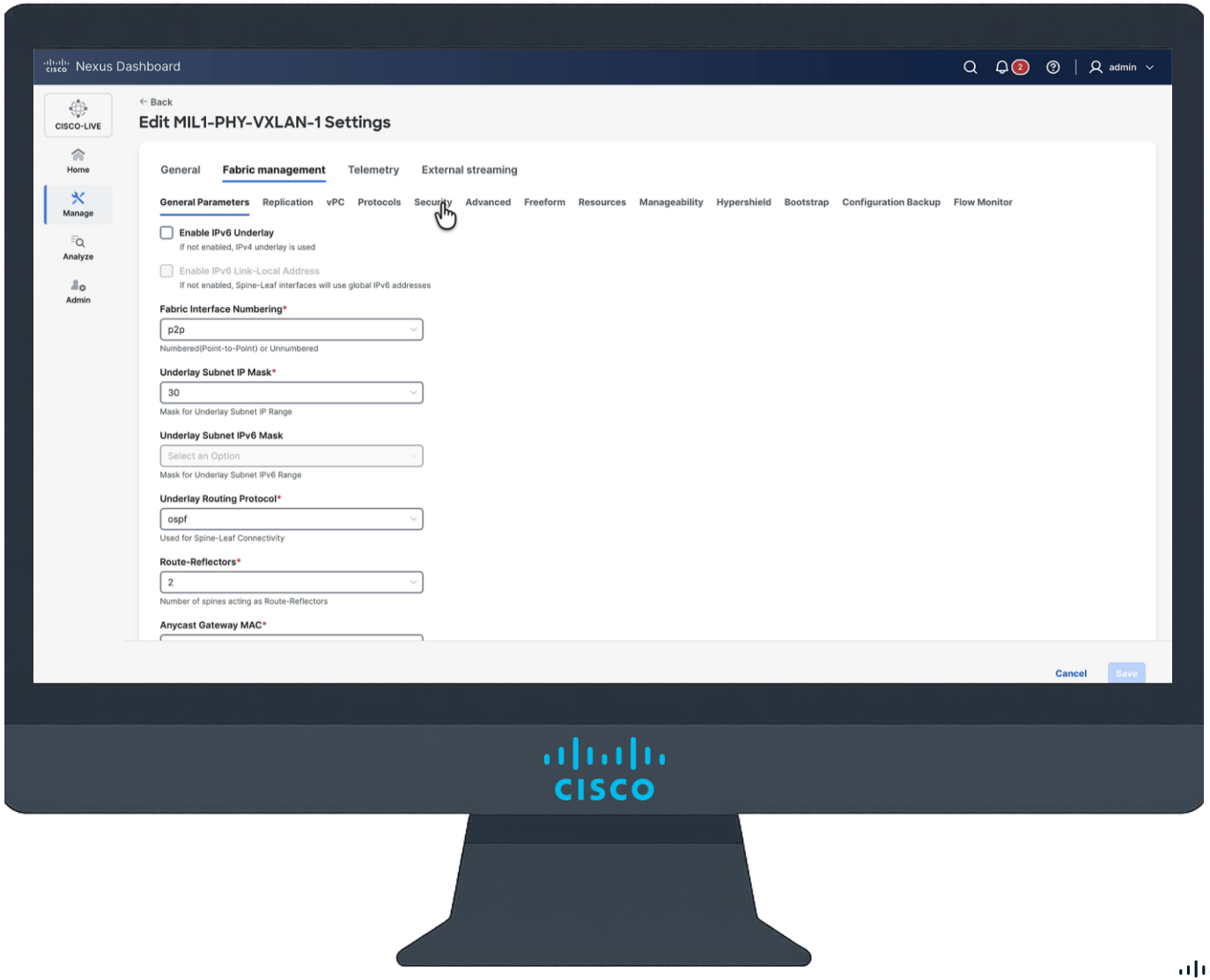
Note: Demos and Screenshots based on ND 4.2 beta

cisco

Group Policy Option

Controller Requirements

- Nexus Dashboard is highly recommended but optional
- Support for GPO added in ND 3.2
- Seamless workflows to help administrators define the Data Center security posture
- Single-Site and Multi-Site supported
- Requires “cli” overlay mode, “config-profiles” are not supported
  - Migration soon available! (**ND 4.2)**
- Day-2 tools to monitor status, forwarding and counters



Note: Demos and Screenshots based on ND 4.2 beta

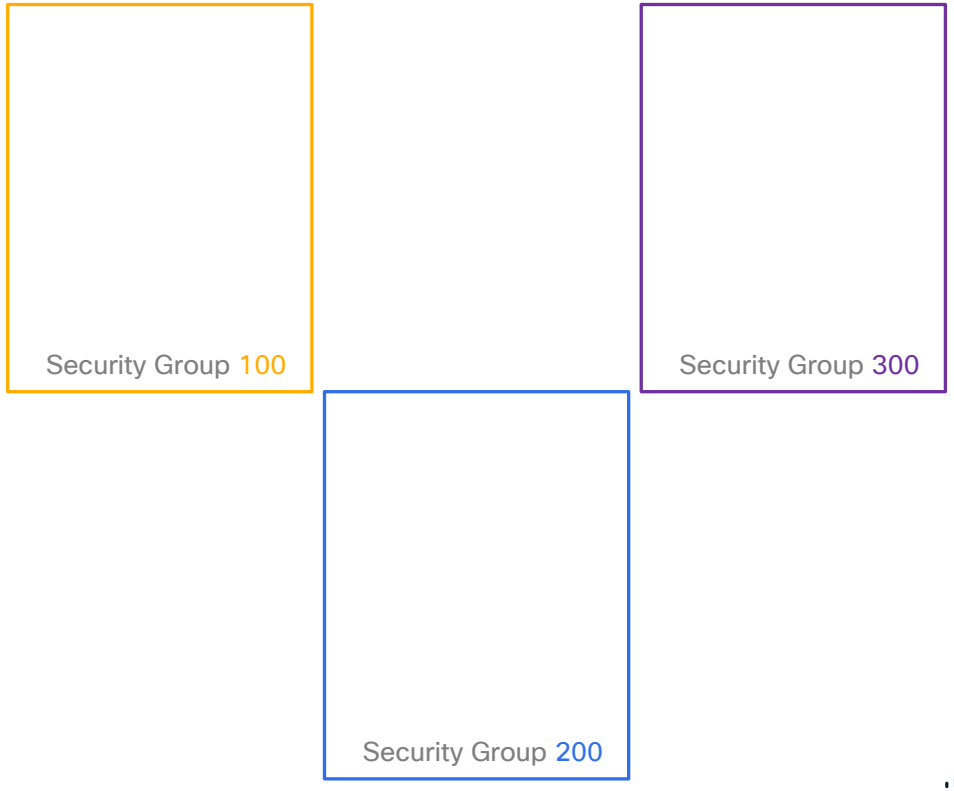
cisco

GPO Review

Group Policy Option Fundamentals

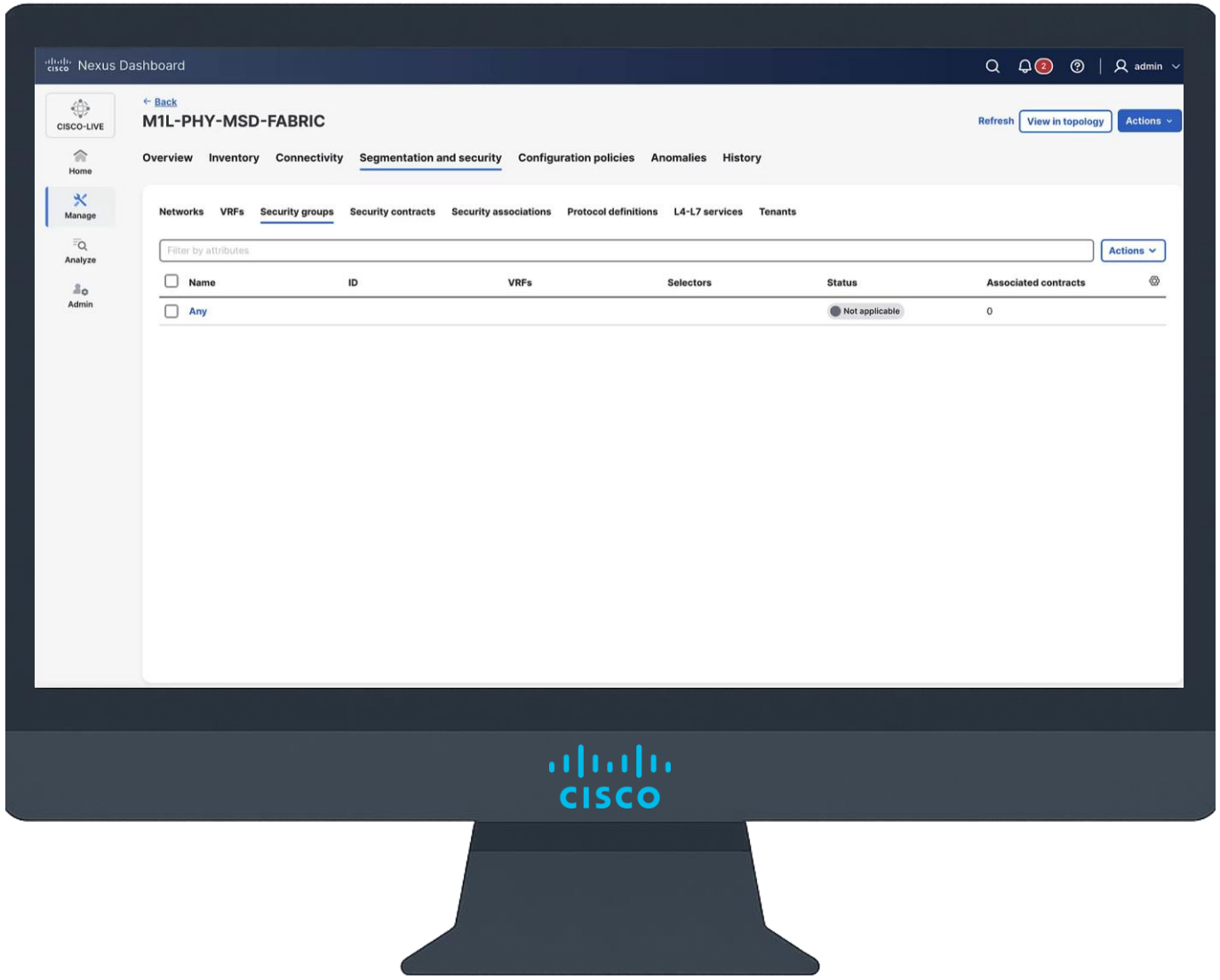
Group Definition

- Security Groups are containers that will include one or more end-hosts or networks with the same security requirements
- Security Groups must be configured with a 16 bit ID called Security Group Tag (SGT), reserved ranges:
  - 0 – 15
  - a_n=130+256·n [130,386,642...65410]
- IP traffic inside the same Security Group always allowed
- IP traffic across different Security Groups must be enforced
- Common reserved SGs:
  - 0 – for any non classified address, also refer to any
  - 1 – for default type-5 routes of directly connected networks
  - 15 – prefixes learned from GPO unaware sites



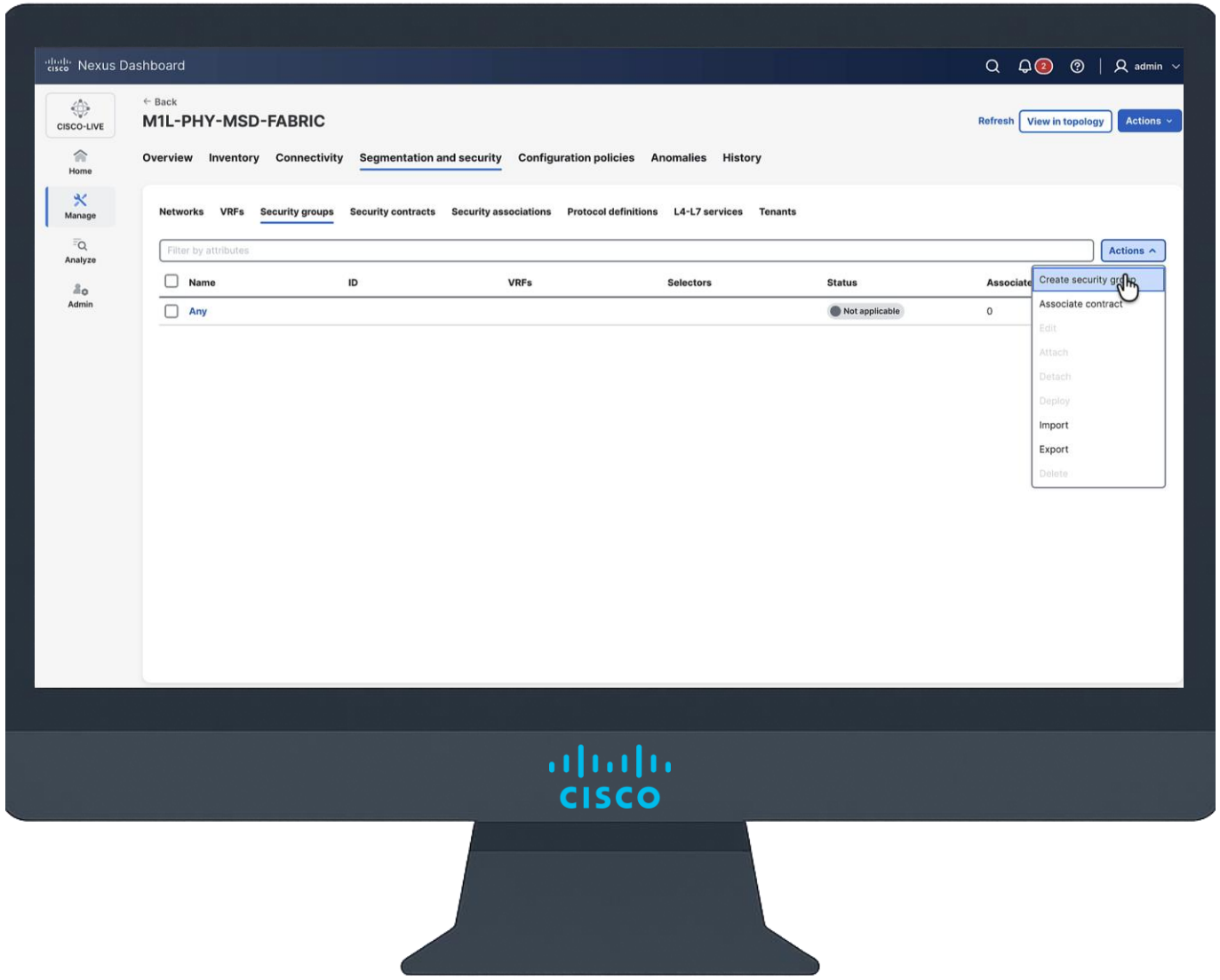
Group Policy Option Fundamentals

Nexus Dashboard - Security Groups



Group Policy Option Fundamentals

Nexus Dashboard - Security Groups

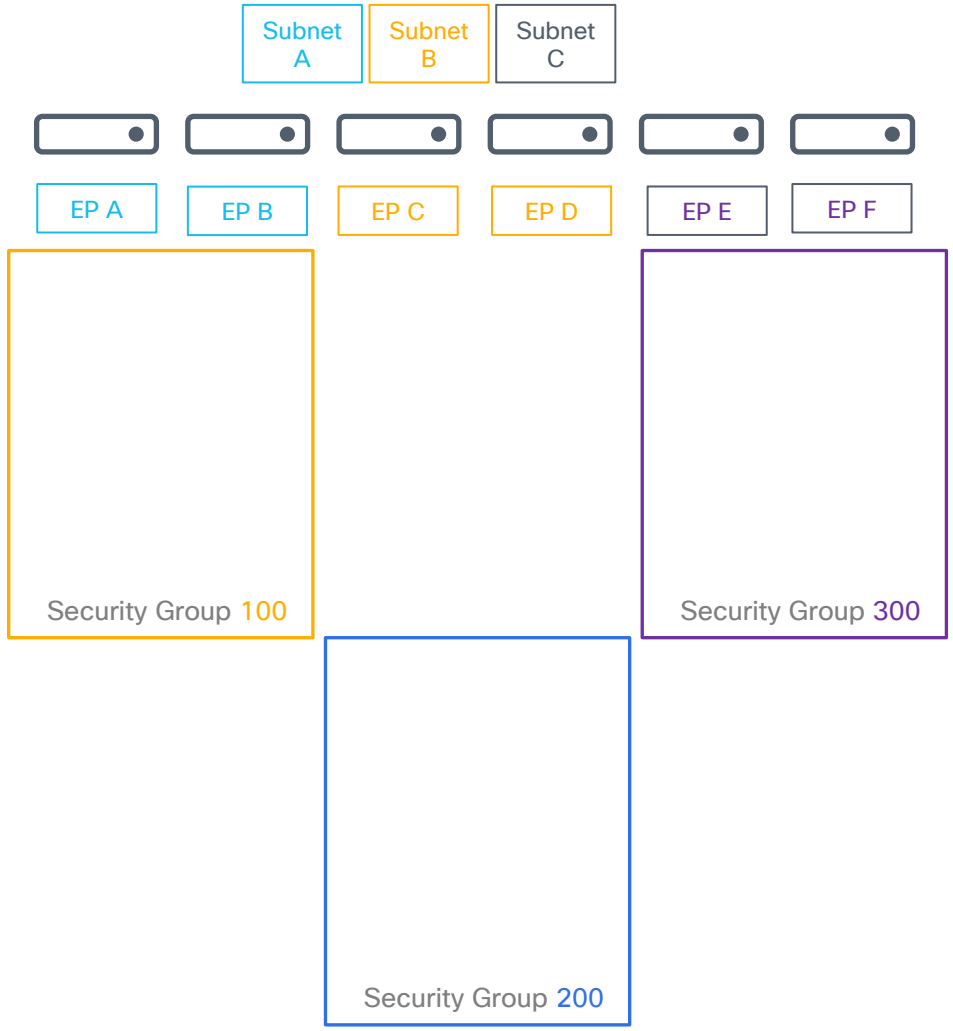


cisco

Group Policy Option Fundamentals

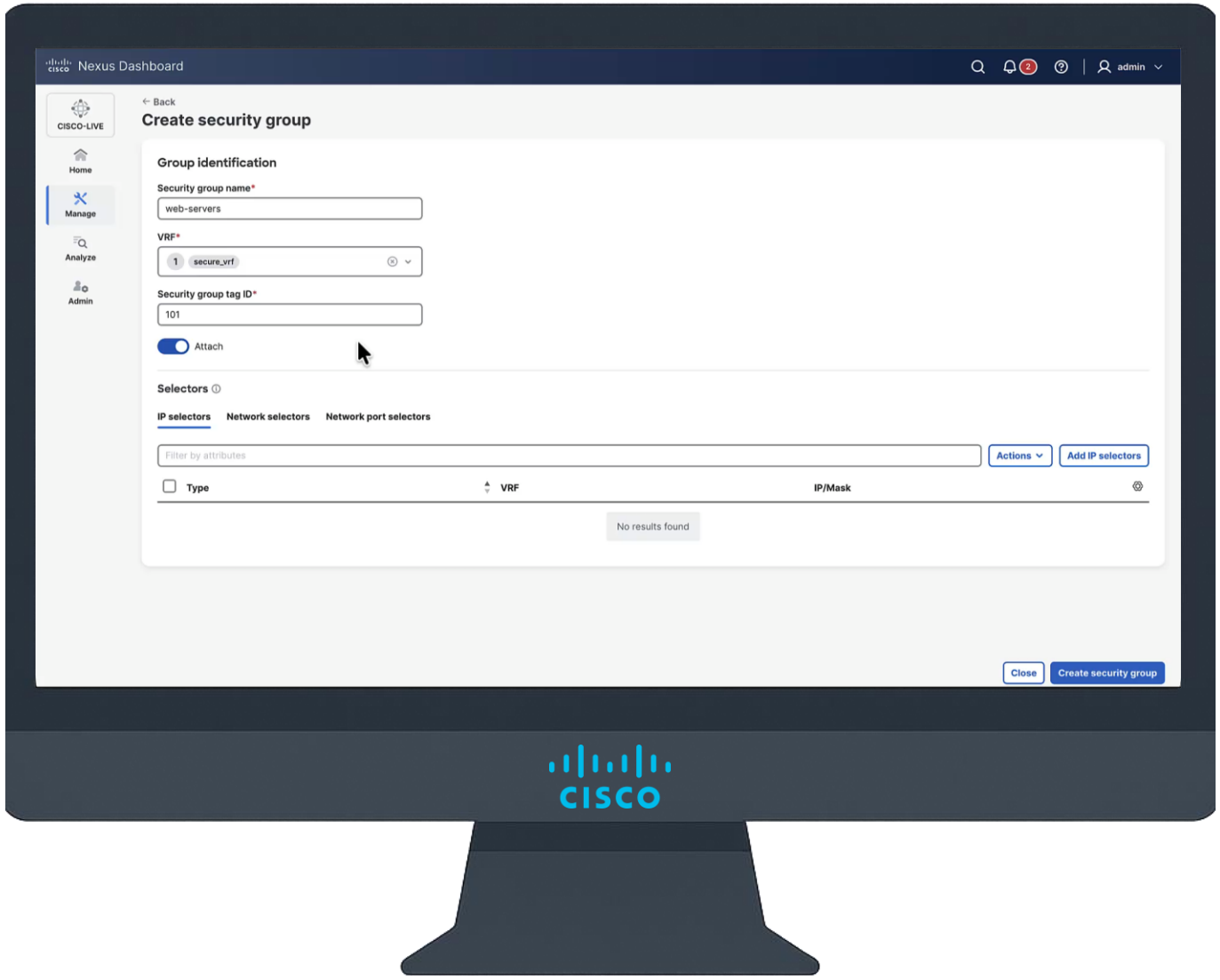
Security Group Classifiers

- Classification, is done in CLI and depends on resource type
  - Connected Endpoints:
    - IP based classification
      - LPMs (including host-routes)



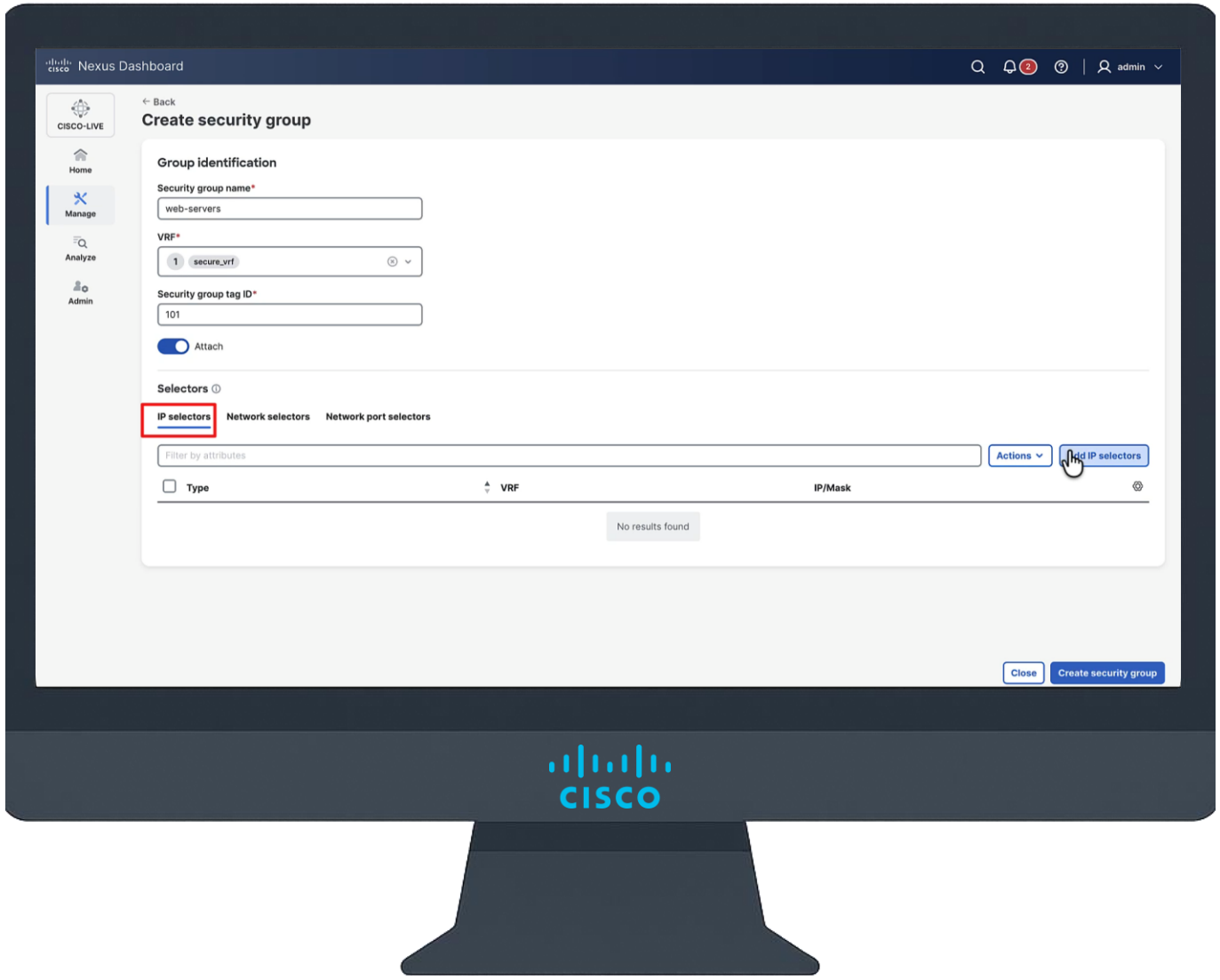
Group Policy Option Fundamentals

Nexus Dashboard – IP Classifiers



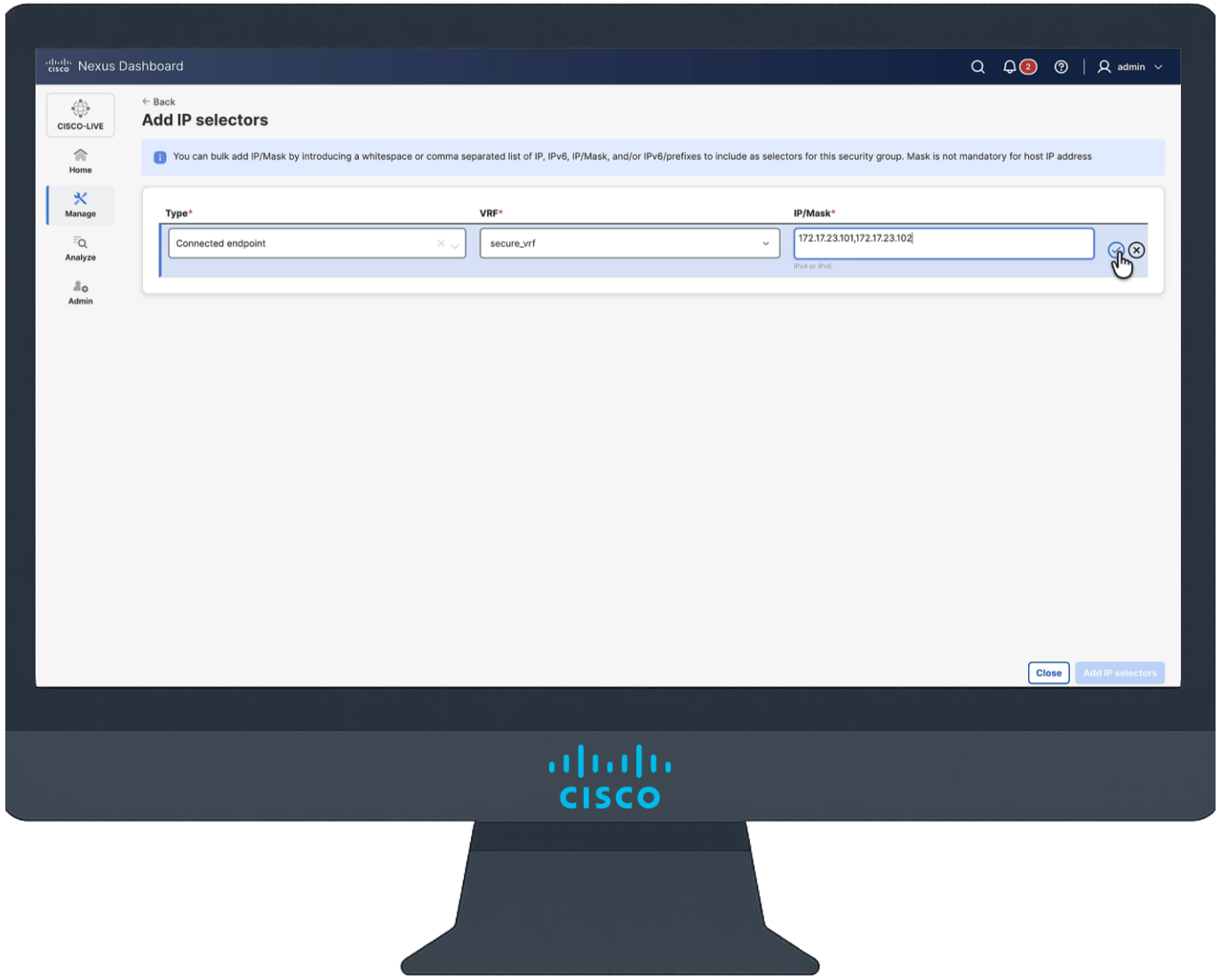
Group Policy Option Fundamentals

Nexus Dashboard – IP Classifiers



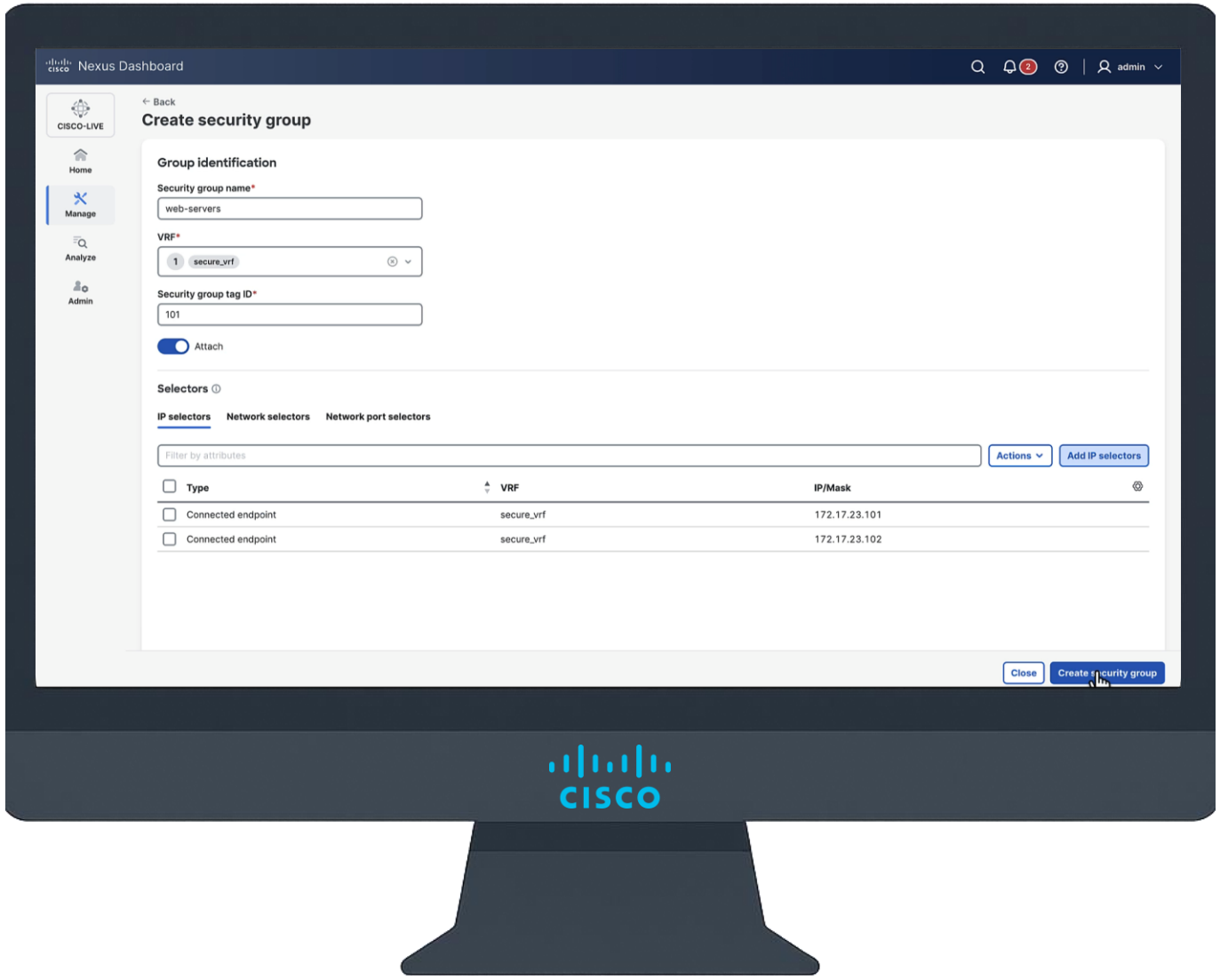
Group Policy Option Fundamentals

Nexus Dashboard – IP Classifiers



Group Policy Option Fundamentals

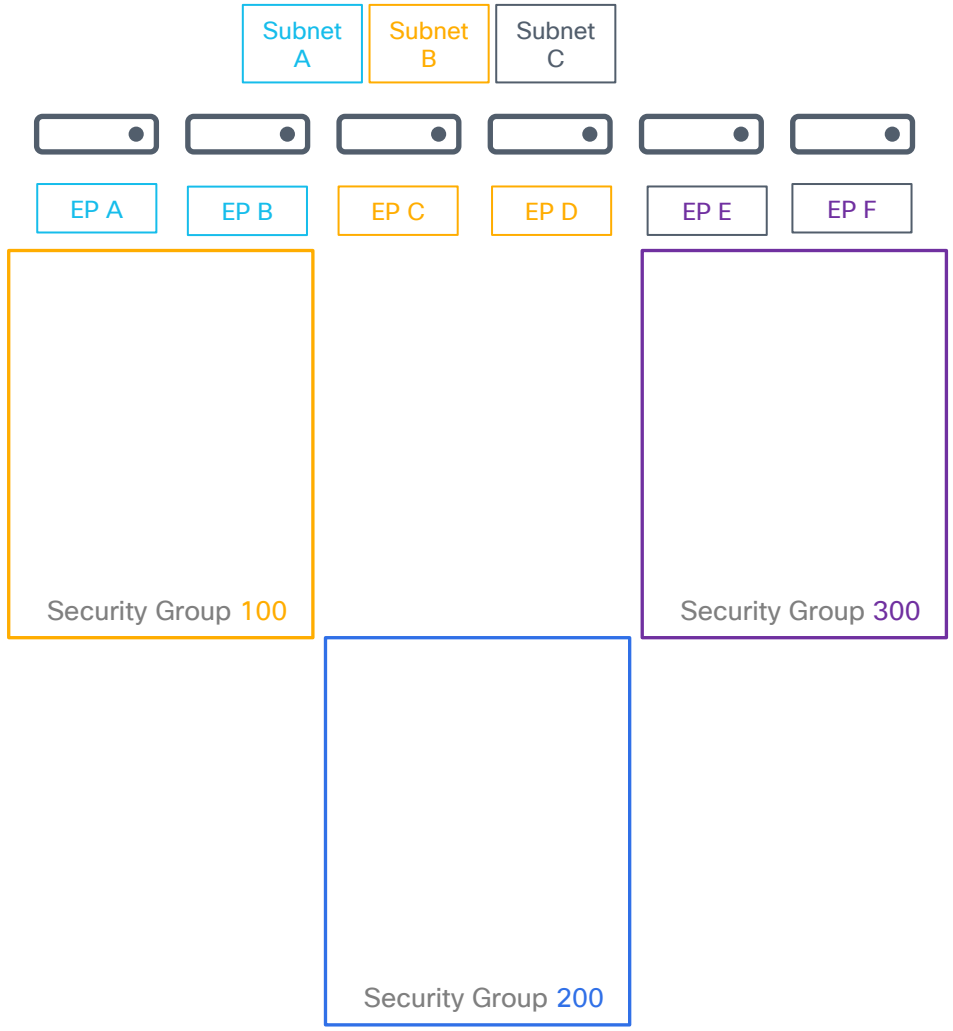
Nexus Dashboard – IP Classifiers



Group Policy Option Fundamentals

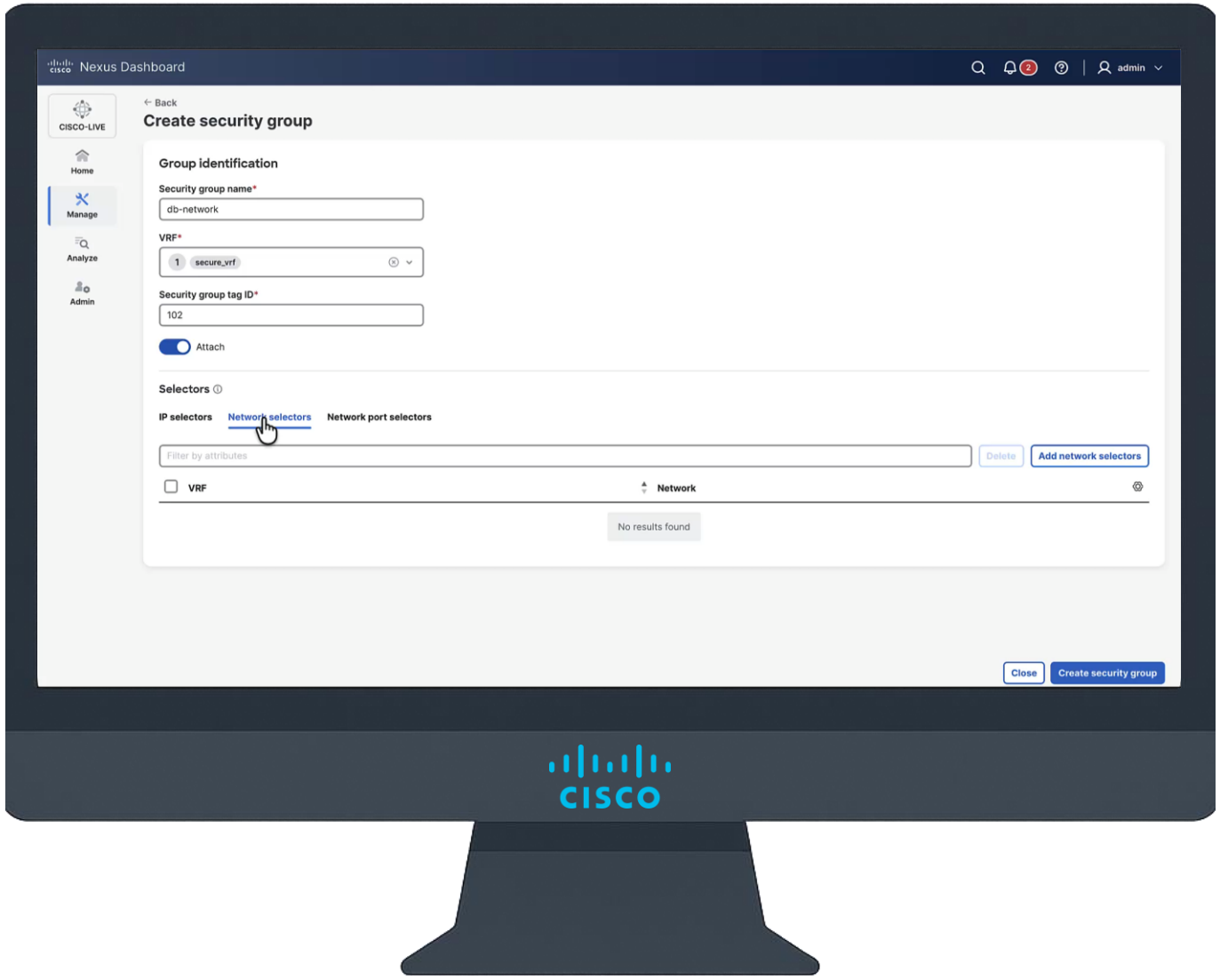
Security Group Classifiers

- Classification, is done in CLI and depends on resource type
  - Connected Endpoints:
    - IP based classification
      - LPMs (including host-routes)
    - VLAN based classification, optionally with port
    - MAC based classification (not yet in Nexus Dashboard)



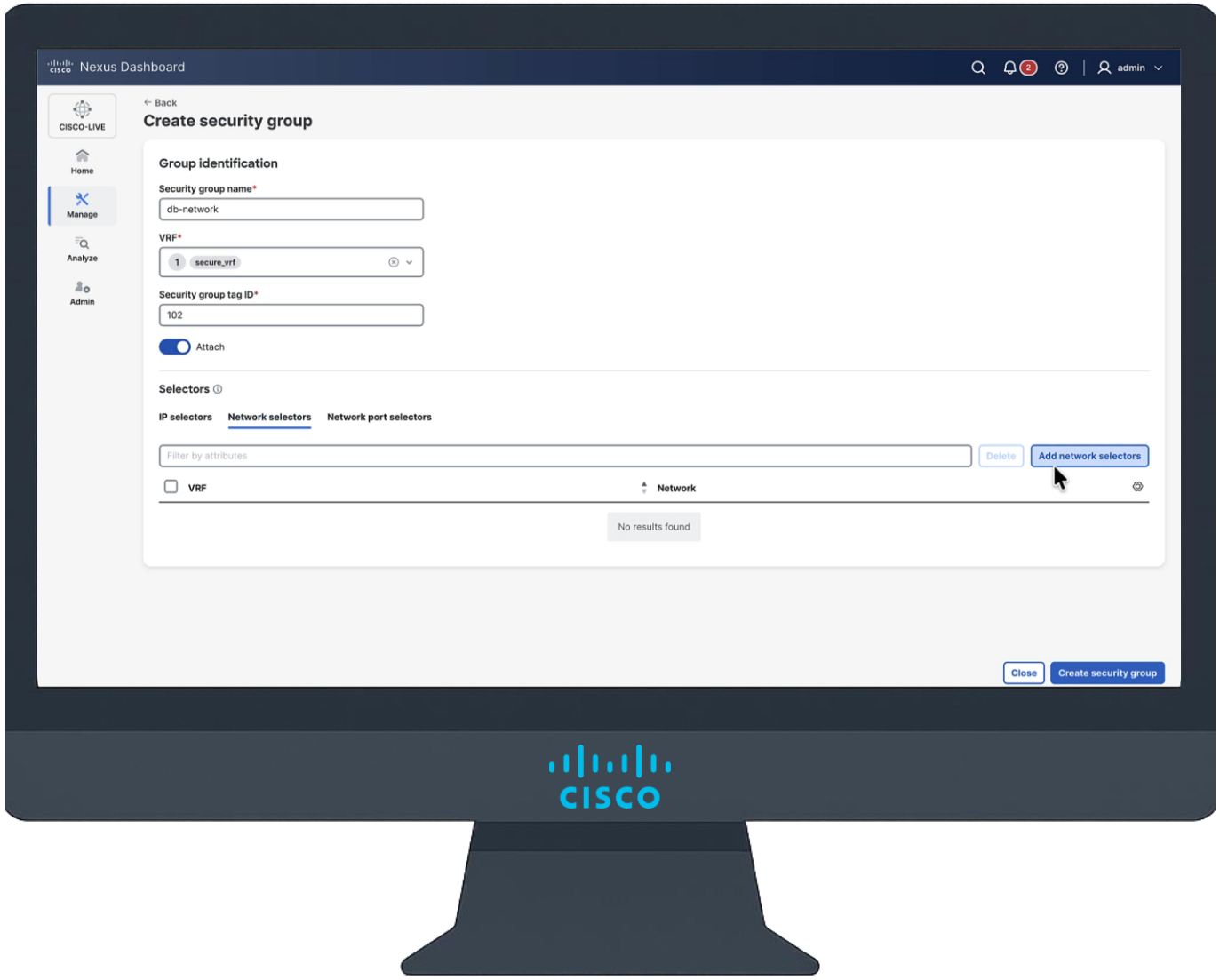
Group Policy Option Fundamentals

Nexus Dashboard - Network Classifier



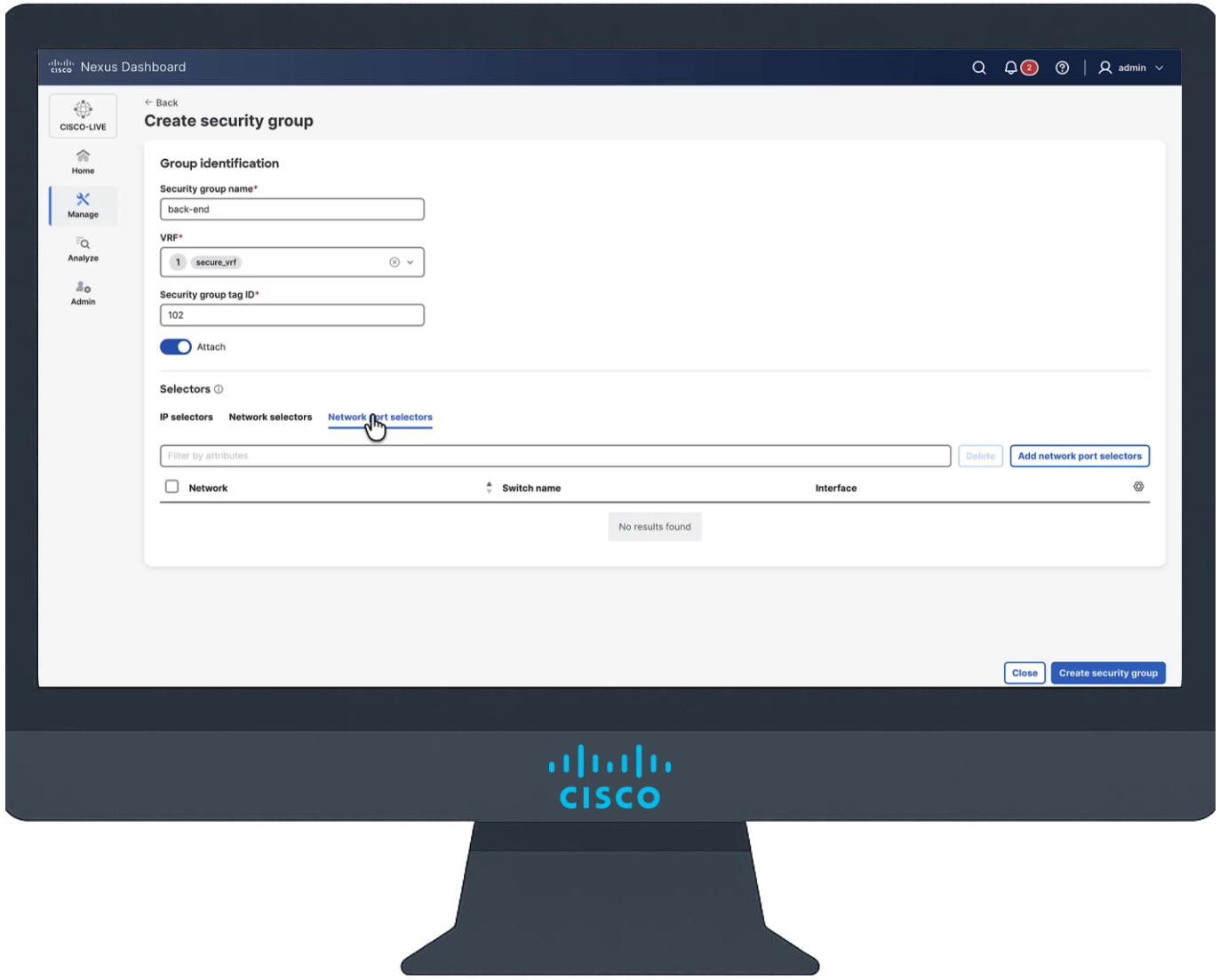
Group Policy Option Fundamentals

Nexus Dashboard - Network Classifier



Group Policy Option Fundamentals

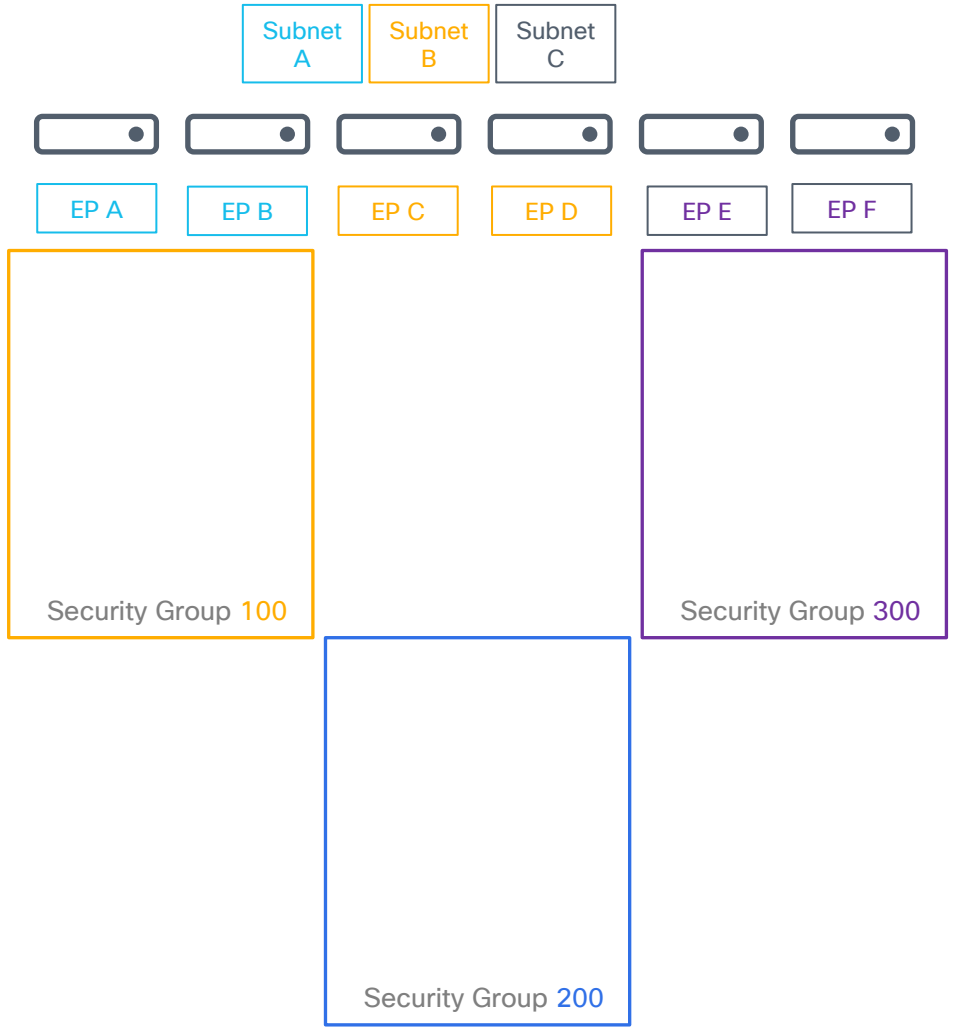
Nexus Dashboard – Network, Port Classifier



Group Policy Option Fundamentals

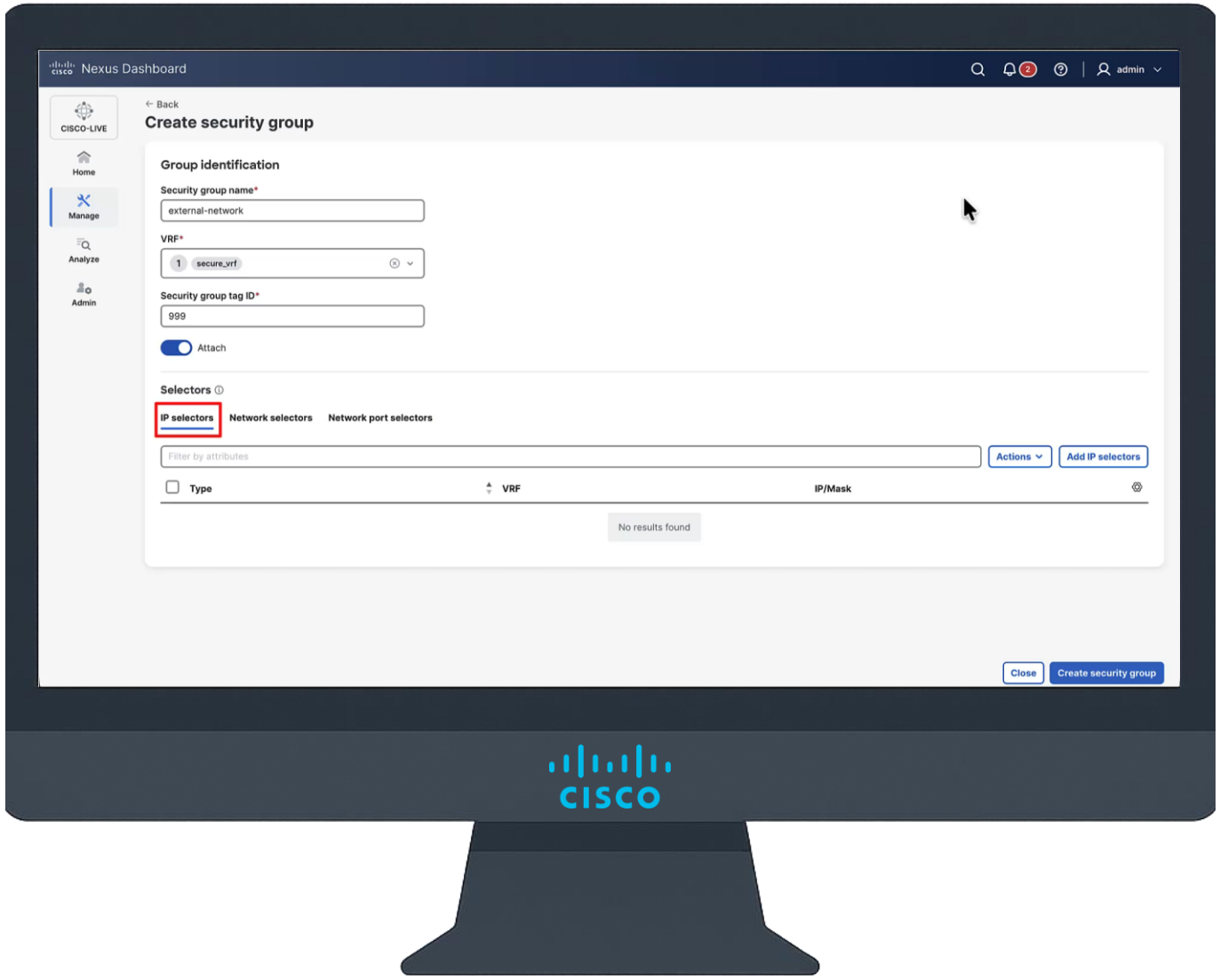
Security Group Classifiers

- Classification, is done in CLI and depends on resource type
  - Connected Endpoints:
    - IP based classification
      - LPMs (including host-routes)
    - VLAN based classification, optionally with port
    - MAC based classification (not yet in Nexus Dashboard)
  - External Networks
    - IP Based Classification
      - LPMs



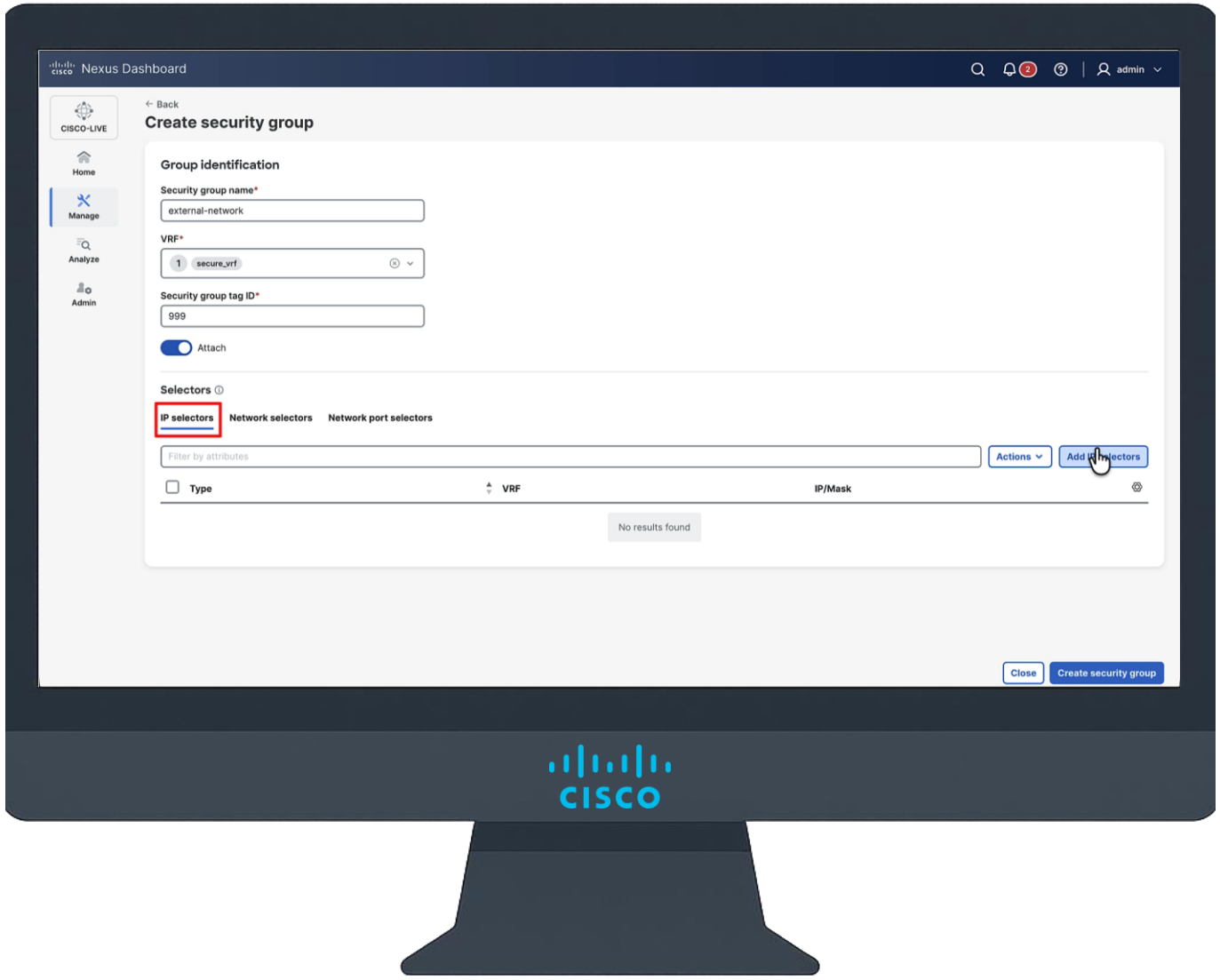
Group Policy Option Fundamentals

Nexus Dashboard – External Network Classifier



Group Policy Option Fundamentals

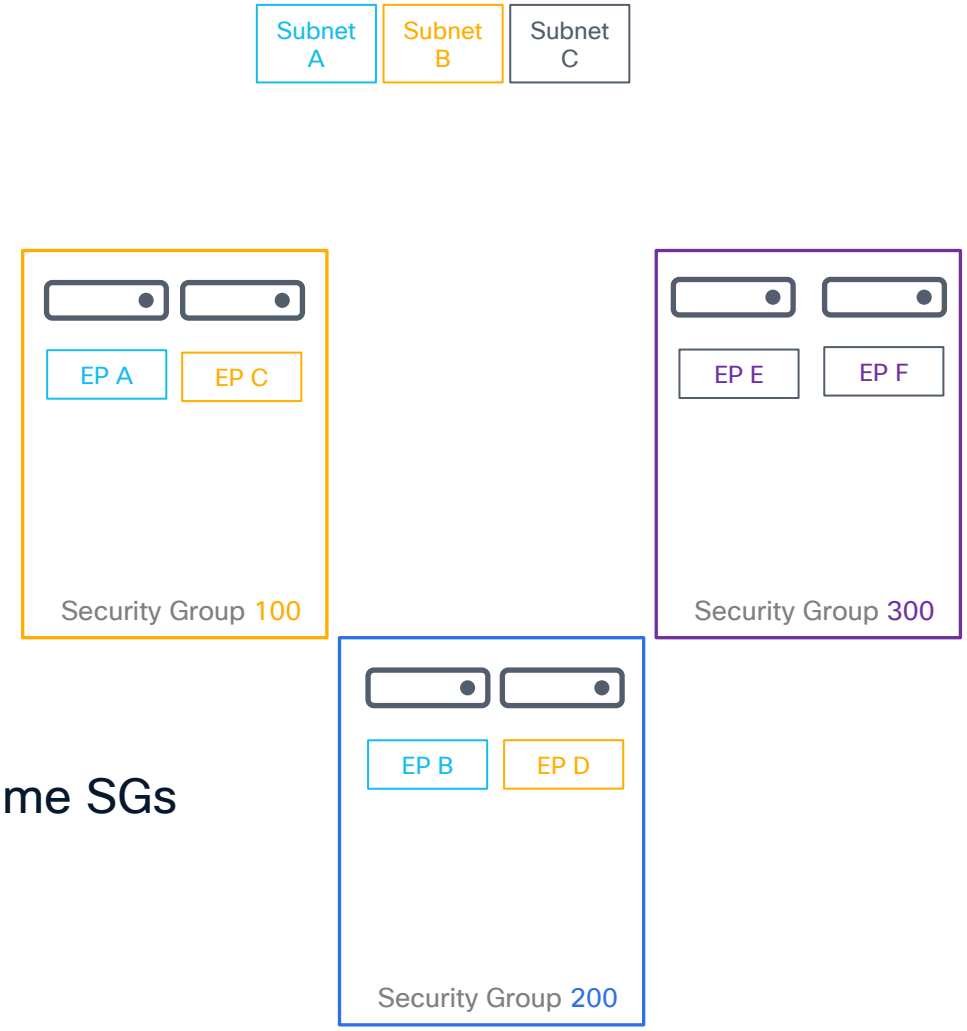
Nexus Dashboard – External Network Classifier



Group Policy Option Fundamentals

Security Group Classifiers

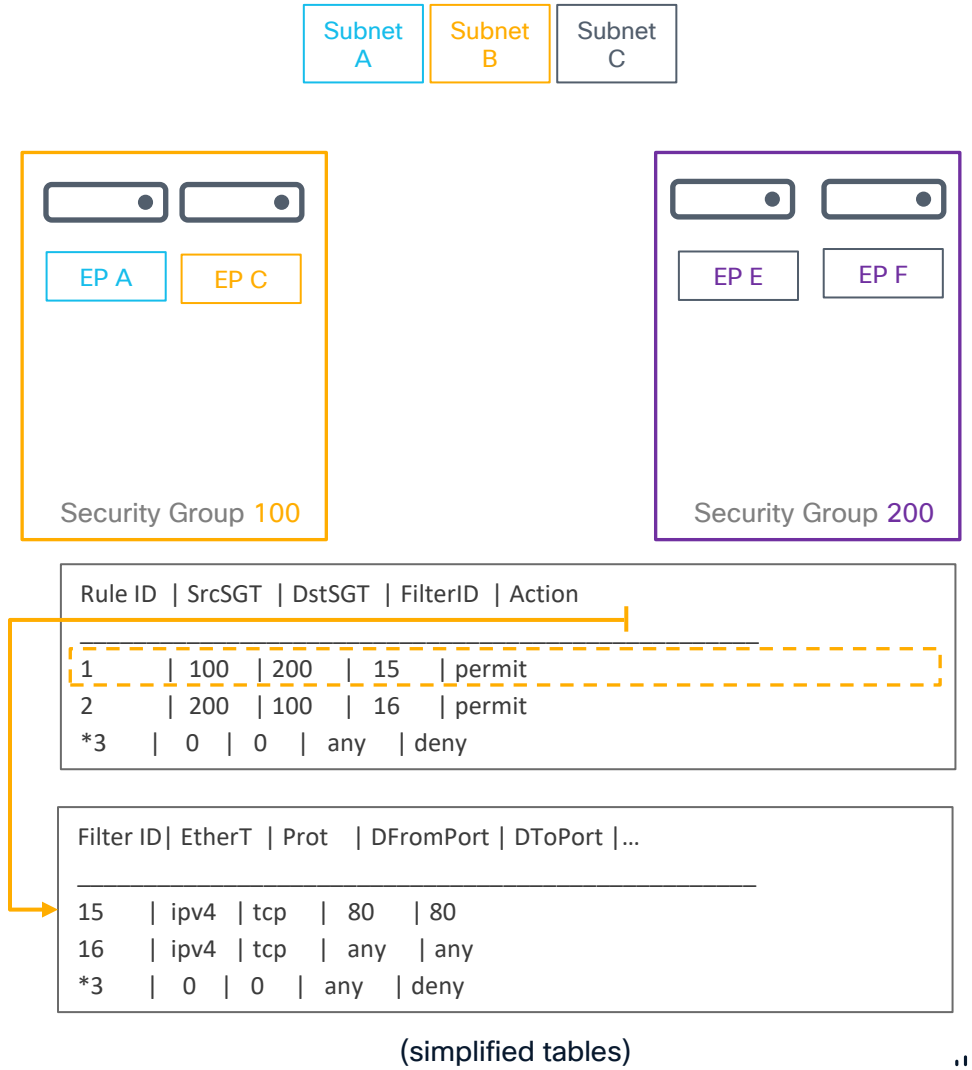
- Classification, is done in CLI and depends on resource type
  - Connected Endpoints:
    - IP based classification
      - LPMs (including host-routes)
    - VLAN based classification, optionally with port
    - MAC based classification (not yet in Nexus Dashboard)
  - External Networks
    - IP Based Classification
      - LPMs
- Endpoints in the same subnet can be mapped to different or same SGs
- Endpoints in different subnets can be mapped to the same SG
- Resources can be part of a single SG



Group Policy Option Fundamentals

Traffic Enforcement

- Traffic enforcement is done by the VTEPs
- Every packet is evaluated in a security-rule table build based on configurations that contains records(SGACLs) to identify source and destination SGT and the conditions (protocol, ports etc)
- When a match is found then the correspondent action is applied
- When multiple matches are configured then a priority logic will be used for the tie break
- If a 1:1 match is not found then a catch–all rule will be hit, the action in that case depends on configurations*



(simplified tables)

Group Policy Option Fundamentals

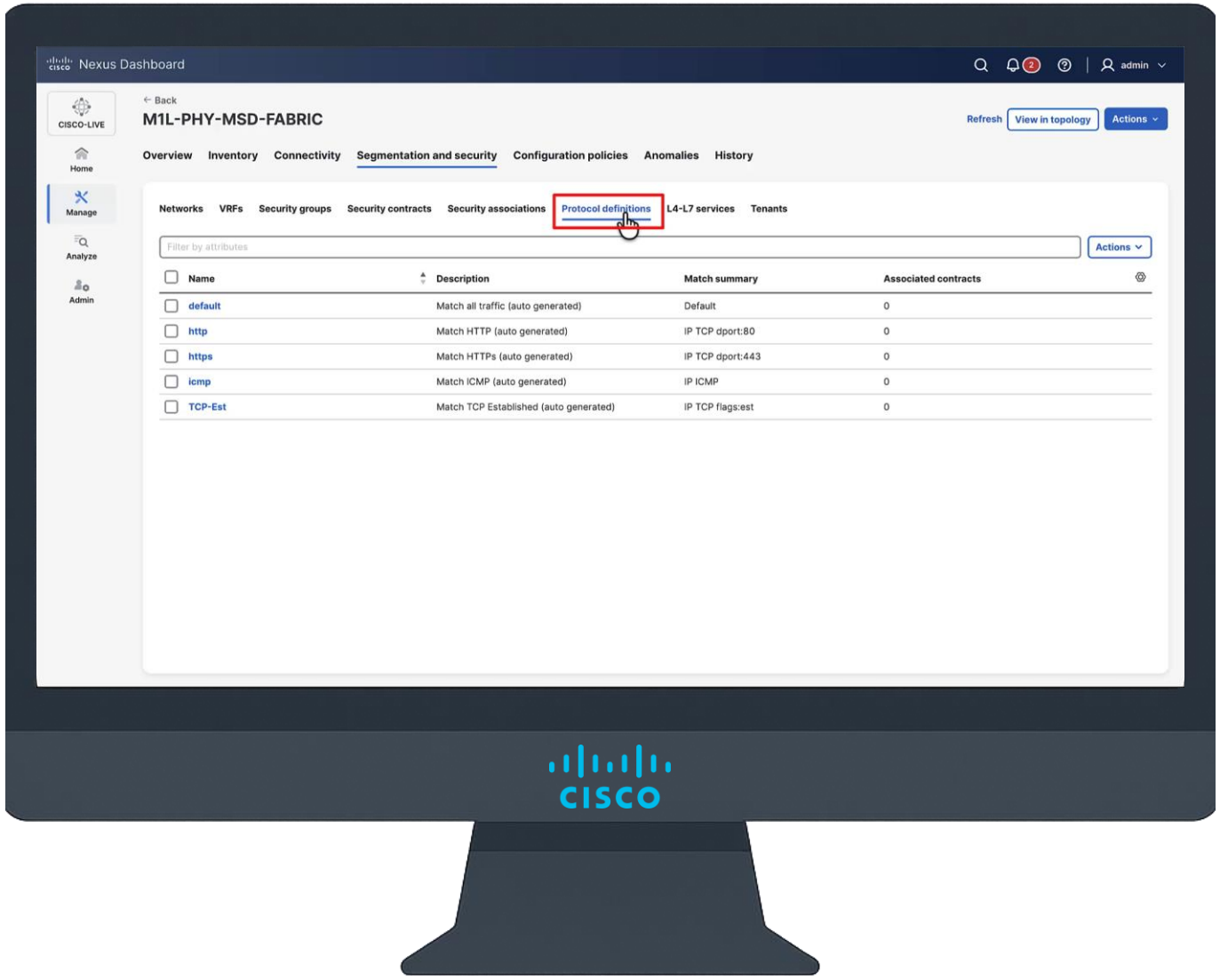
Traffic Enforcement – Filters

- SGACLs always match traffic between a source and a destination Security Group based on a filter
- Filters can include one or more entries that identify the traffic type. Valid options are:
  - IPv4/IPv6 carried protocol
  - TCP/UDP ports
  - TCP flags
  - DSCP
  - Fragments
- Filters are defined with “class-map type security” objects

```
class-map type security match-any TCP-PORT-80
  match ipv4 tcp dport 80

class-map type security match-any TCP-PORT-443
  match ipv4 tcp dport 443

class-map type security match-any MY-APP
  match ipv4 tcp dport 15000 to 15146

class-map type security match-any WEB-TRAFFIC-PORTS
  match ipv4 tcp stateful dport 443
  match ipv4 tcp stateful dport 80
  match ipv4 udp dport 443

class-map type security match-any MANAGEMENT
  match ipv4 tcp dport 3389
  match ipv4 tcp dport 22
```

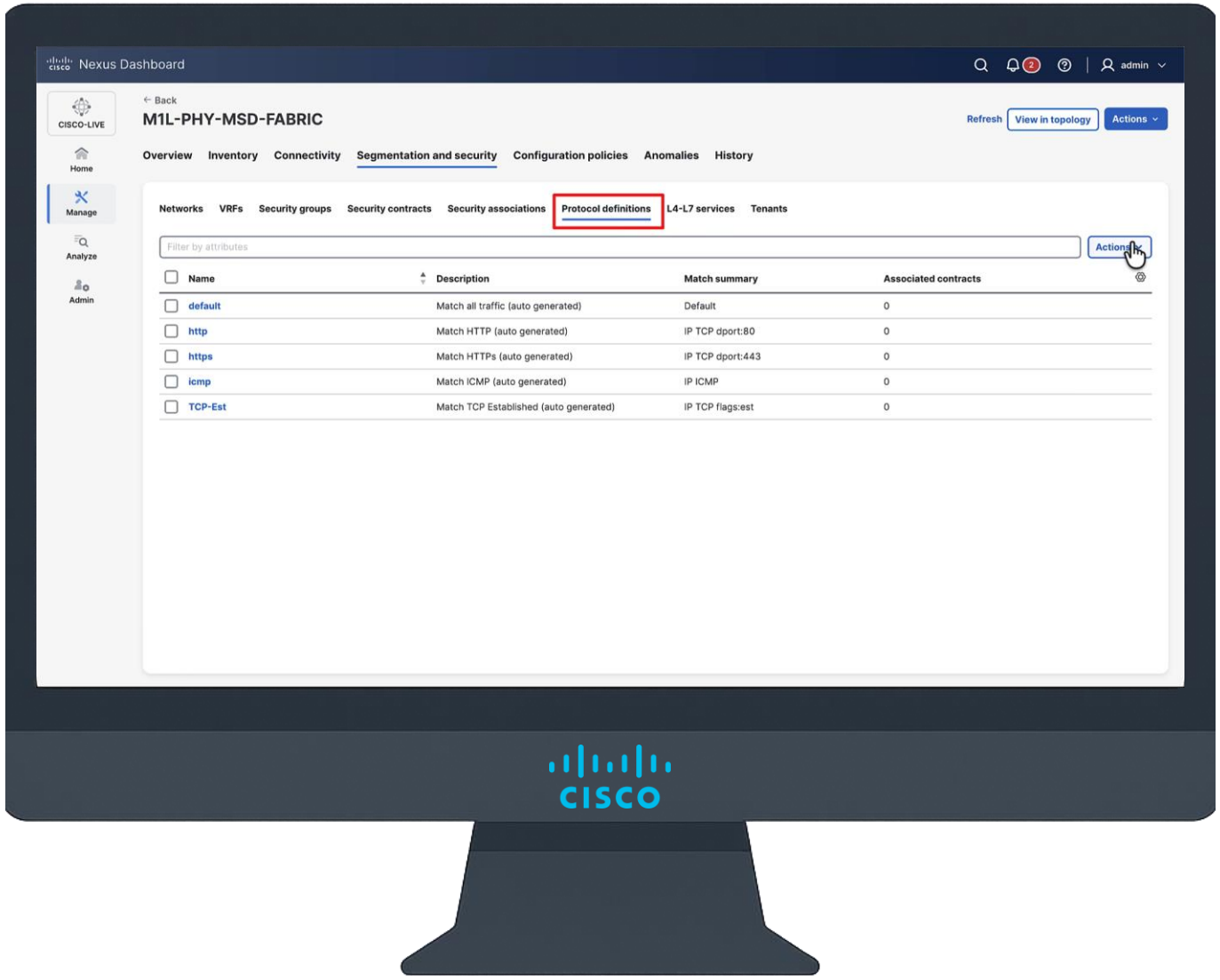
Group Policy Option Fundamentals

Nexus Dashboard - Protocols



Group Policy Option Fundamentals

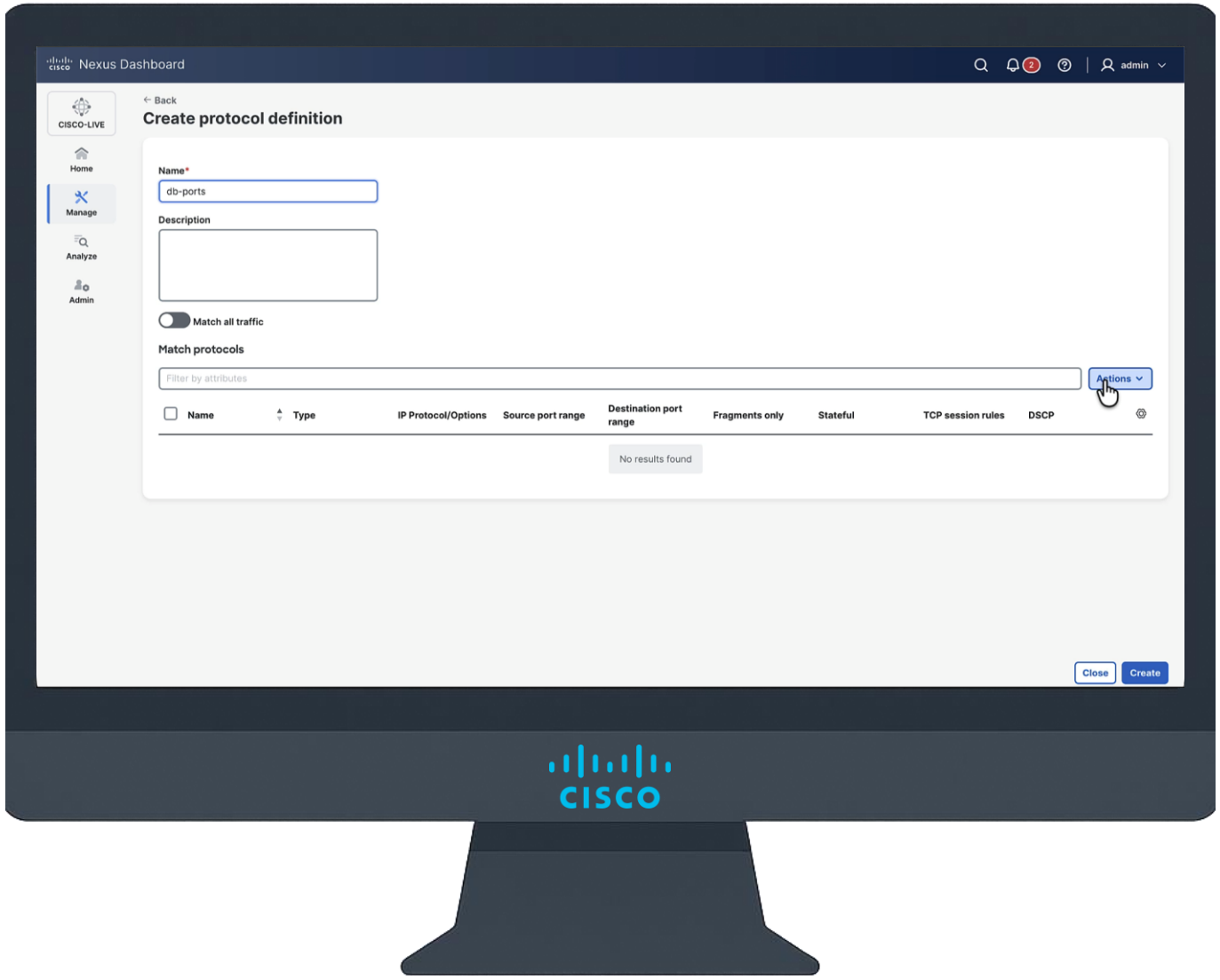
Nexus Dashboard - Protocols



cisco

Group Policy Option Fundamentals

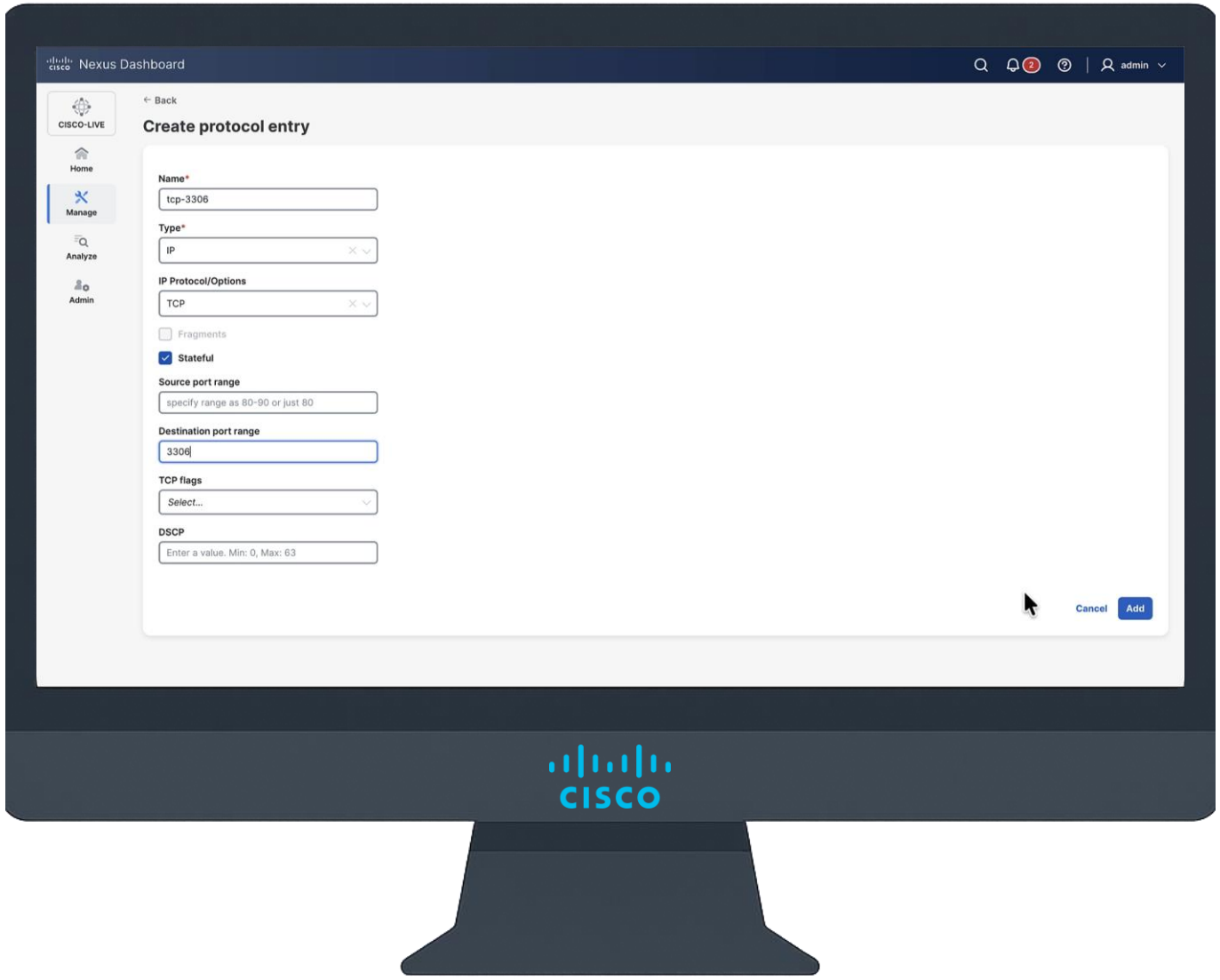
Nexus Dashboard - Protocols



cisco

Group Policy Option Fundamentals

Nexus Dashboard - Protocols



Group Policy Option Fundamentals

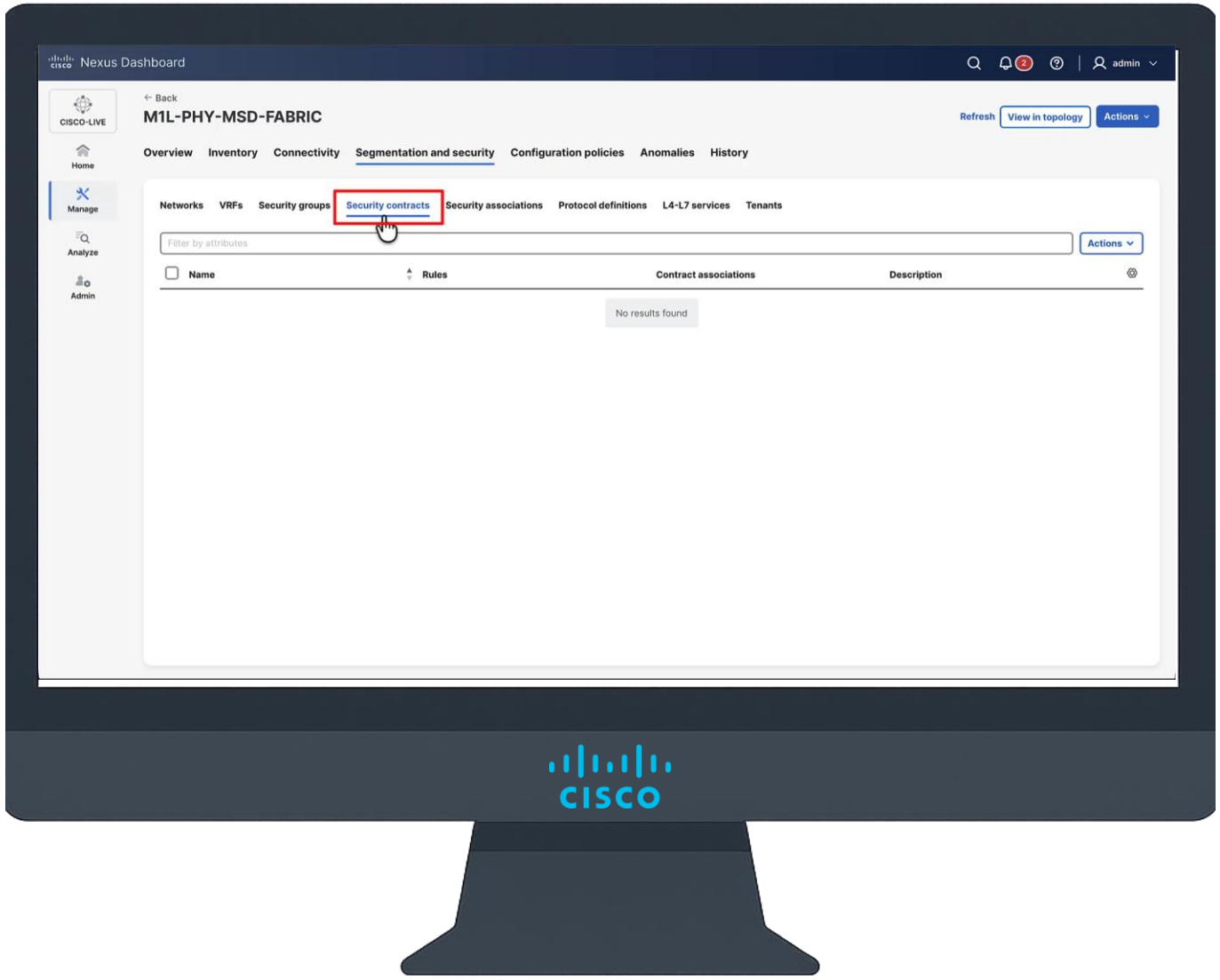
Traffic Enforcement – Policies

- Policies, or contracts, defined the action that will be programmed on the hardware(filter):
  - Permit
  - Deny
  - Redirect to a Service (*service-chain*)
- Multiple filters may be be included in a single policy each one with a different action
- Device can log and track hit counts when the log keyword is used
- Policies can be safely re-used, there is no risk to allow unintended traffic (might make sense to ACI folks)

```
policy-map type security VPN-CLIENTS-TO-ANY
  class TCP-PORT-80
    log
    service-chain WEB-CHAIN-SITE-1
  class MANAGEMENT
    permit
  class default
    log
    deny

policy-map type security ONLY-WEB-PORTS
  class WEB-TRAFFIC-PORTS
    log
    service-chain WEB-CHAIN-SITE-1
class default
    log
    deny
```

Group Policy Option Fundamentals

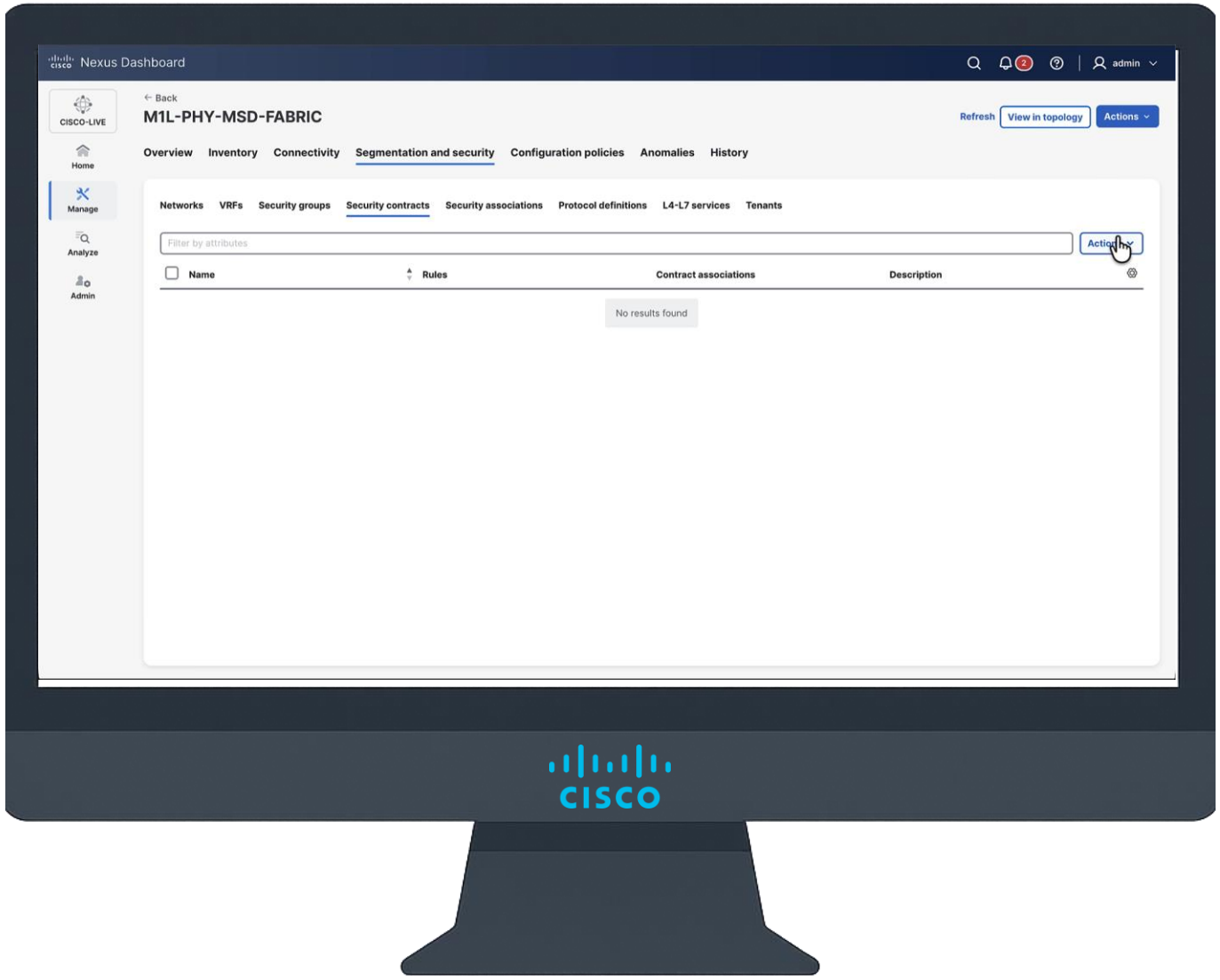
Nexus Dashboard - Contracts



cisco

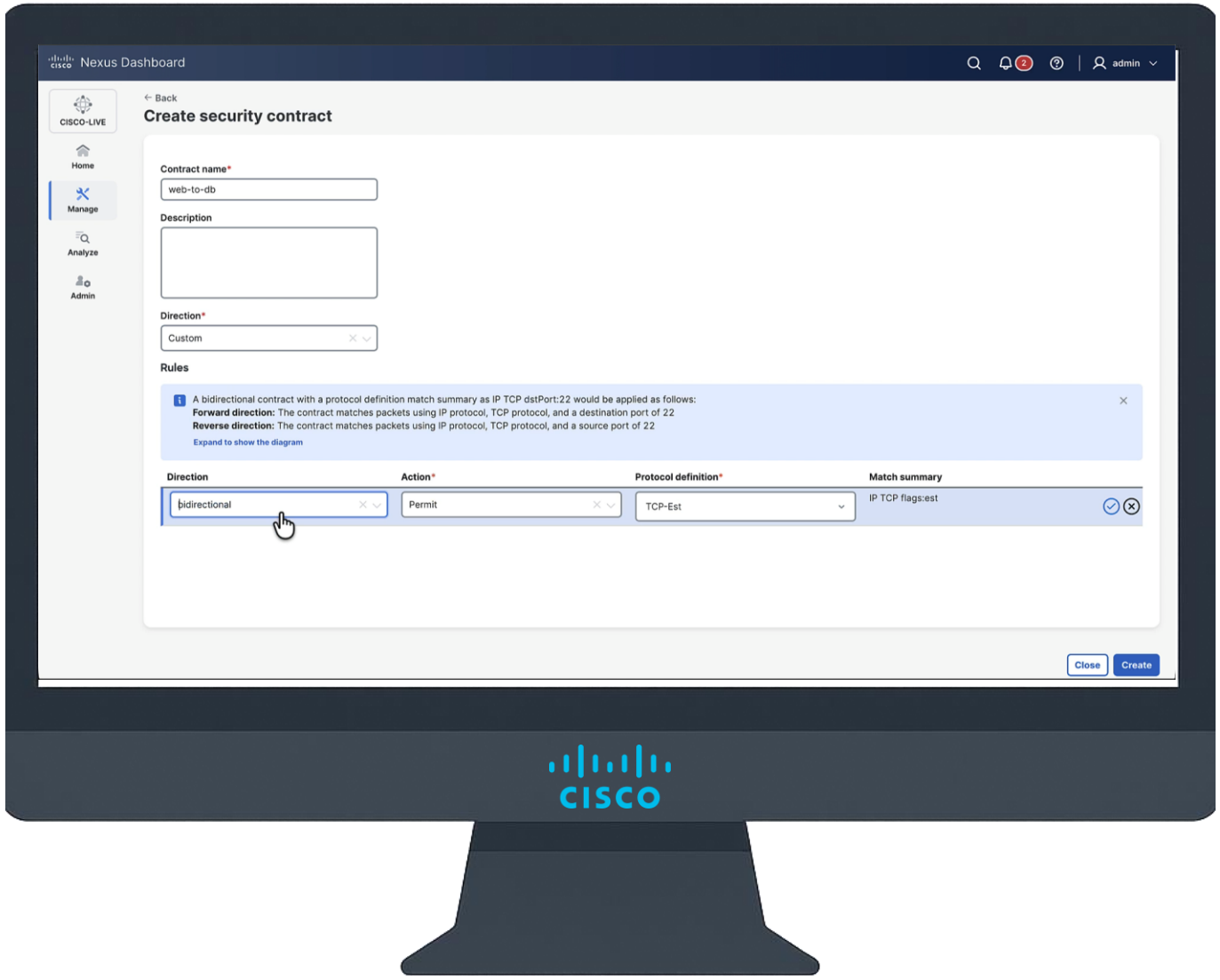
Group Policy Option Fundamentals

Nexus Dashboard - Contracts



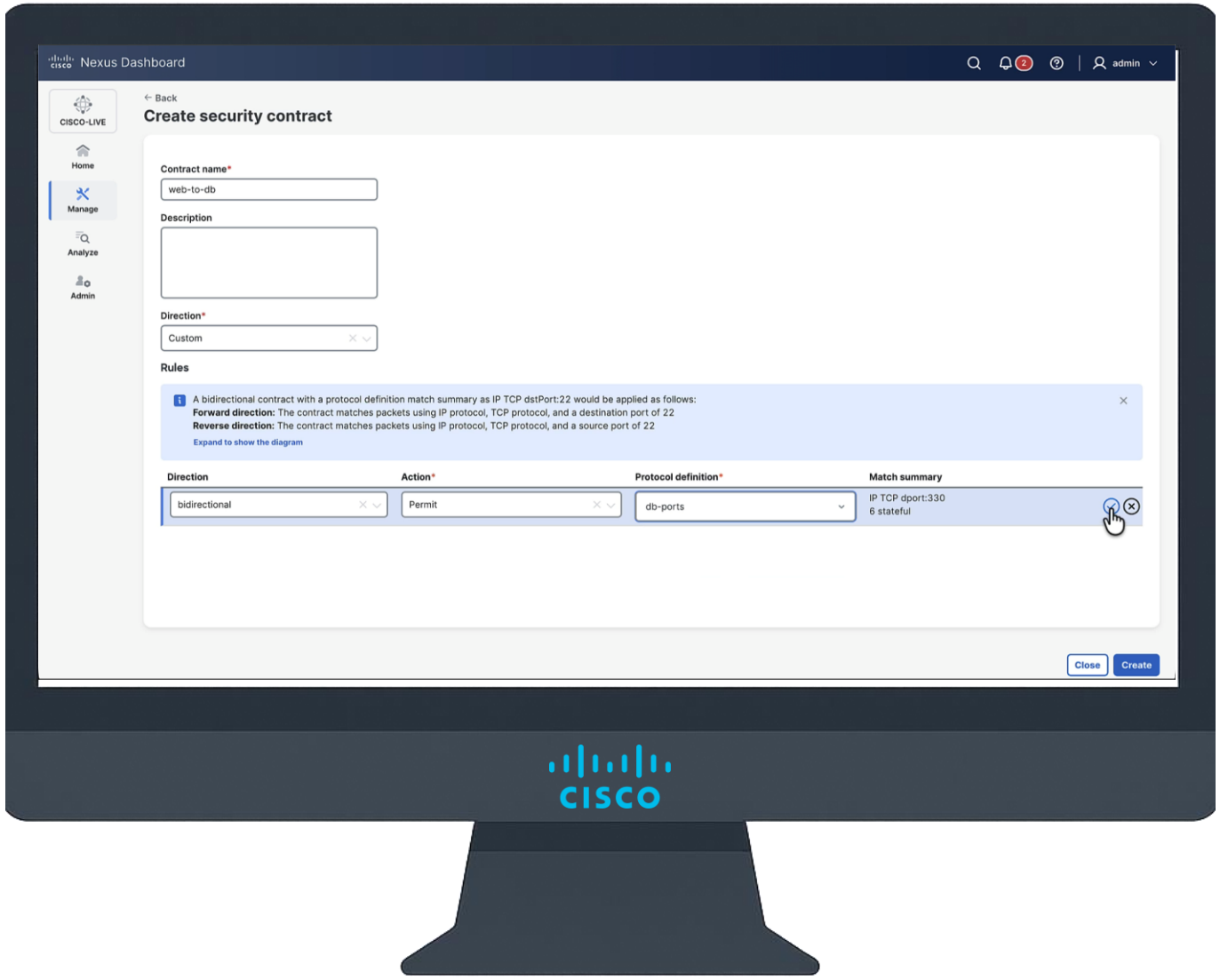
Group Policy Option Fundamentals

Nexus Dashboard - Contracts



Group Policy Option Fundamentals

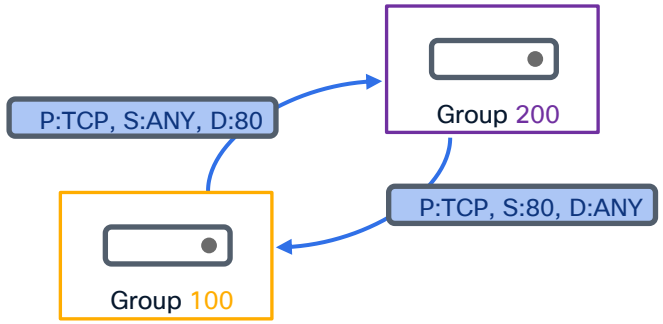
Nexus Dashboard - Contracts



Group Policy Option Fundamentals

Traffic Enforcement – Associations

- Associations set the policy between a source and a destination SGT
- Multiple associations can be defined between the same S-SGT and D-SGT if they refer to a different policy
- Associations can be:
  - Unidirectional
  - Bidirectional (default)
- When an association is bidirectional the switch programs the hardware rule to allow the return traffic

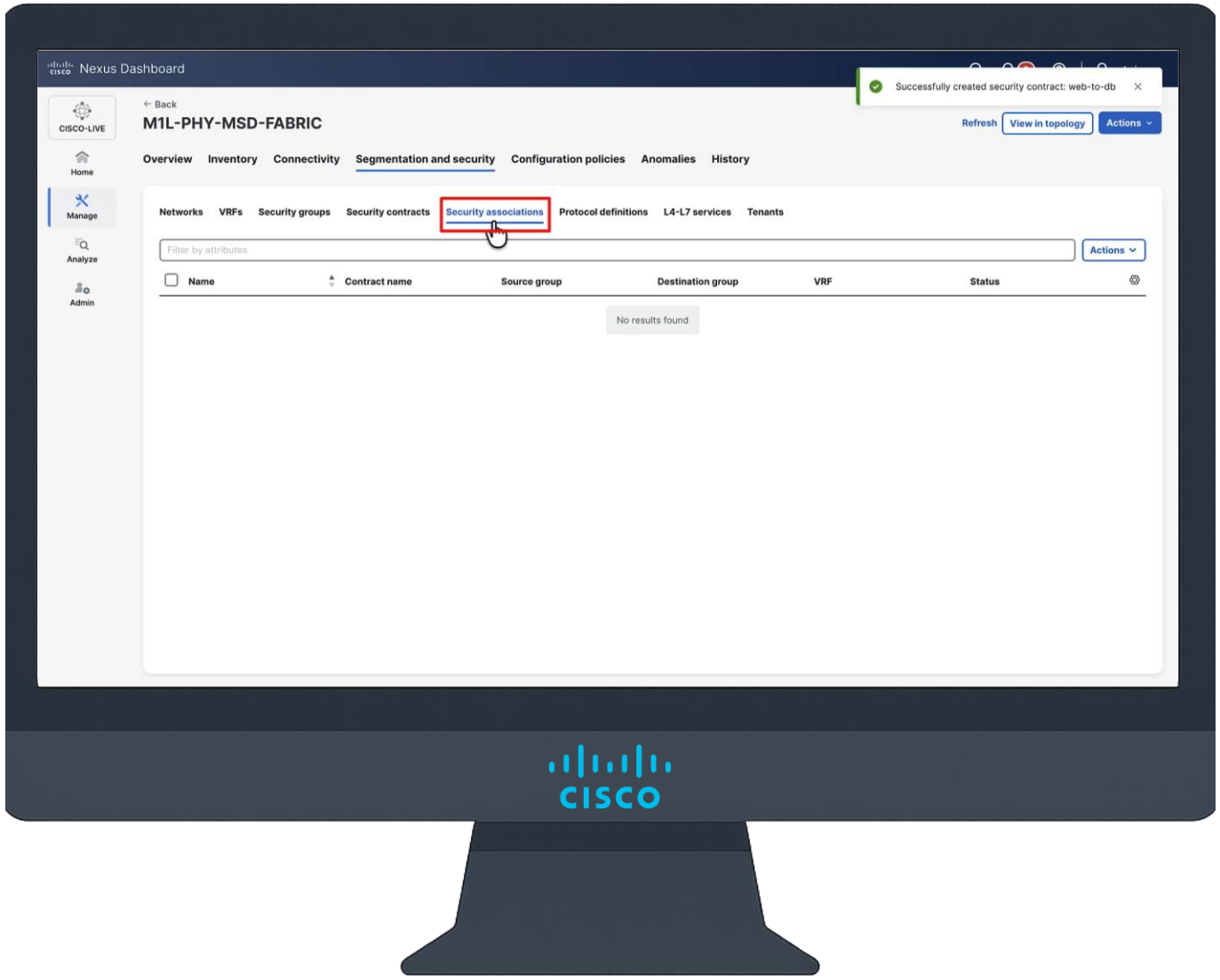



```
vrf context my_vrf
  security contract source 100 destination 200 policy ONLY-TCP-PORT-80 bidir*
```

*default setting

Group Policy Option Fundamentals

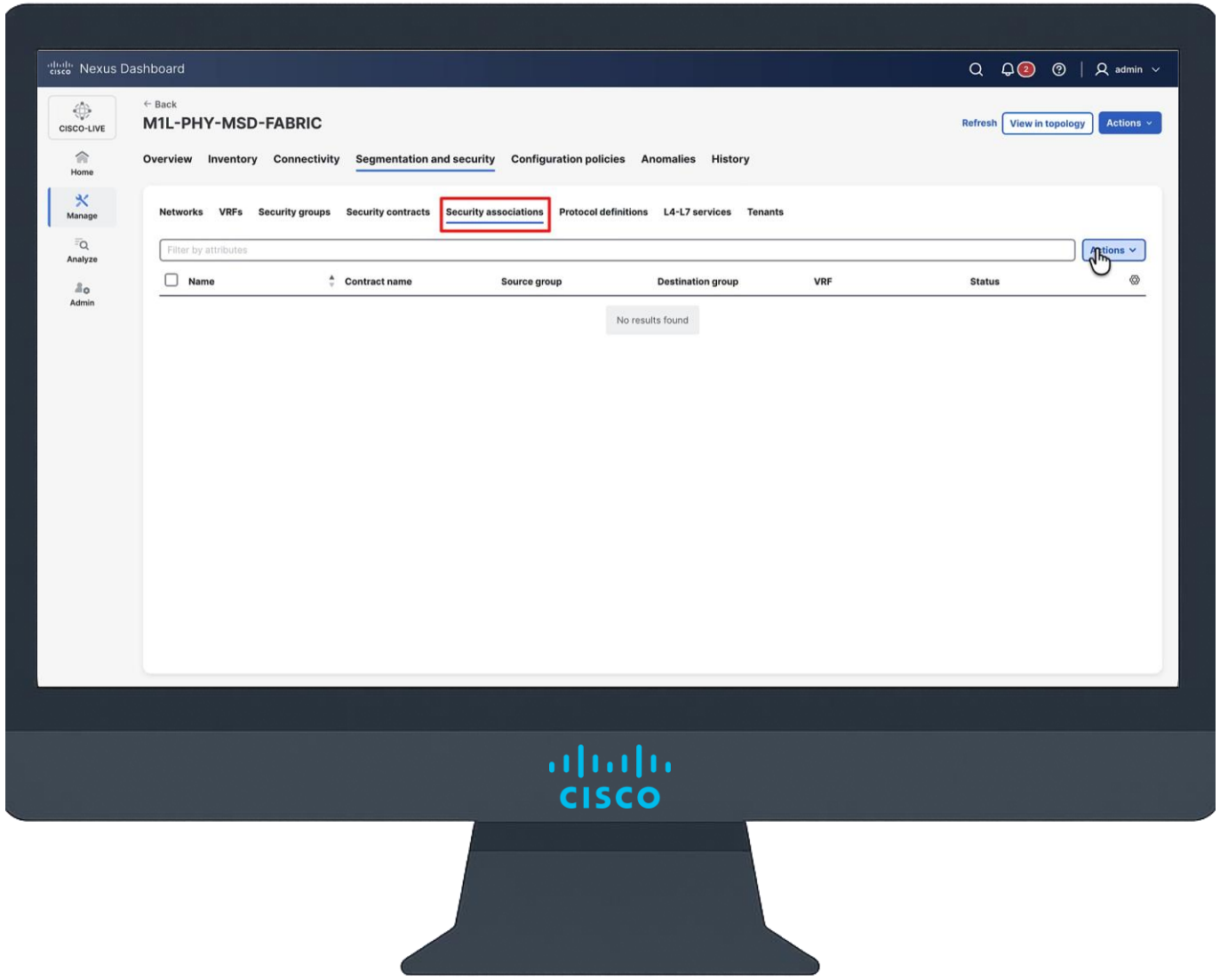
Nexus Dashboard – Associations



cisco

Group Policy Option Fundamentals

Nexus Dashboard – Associations

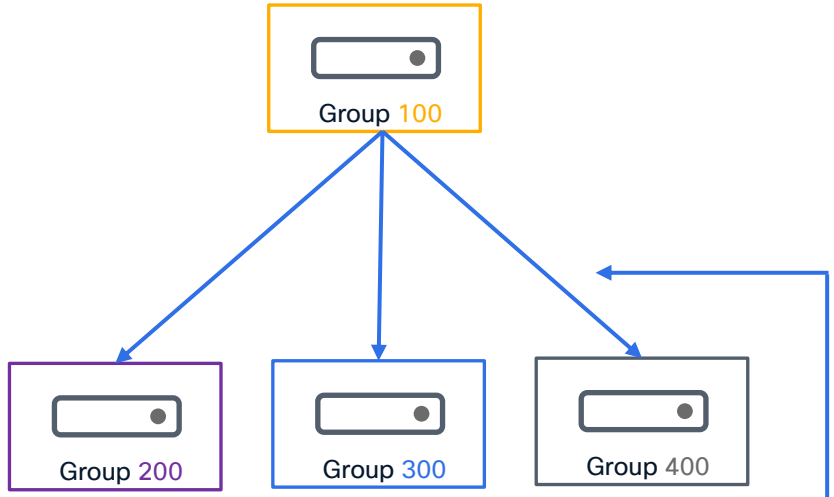


cisco

Group Policy Option Fundamentals

Traffic Enforcement – Associations with Any

- Associations can also be mapped to a special object defined with the **“any”** keyword
- **“Any”** represents all the security-groups part of a VRF
- This allows the administrator to define a single rule when the following communications are required:
  - One to many
  - Many to one
  - Many to Many
- In case of SGACL overlaps, the most specific wins
  - One to One
  - One to Many
  - Many to One
  - Many to Many

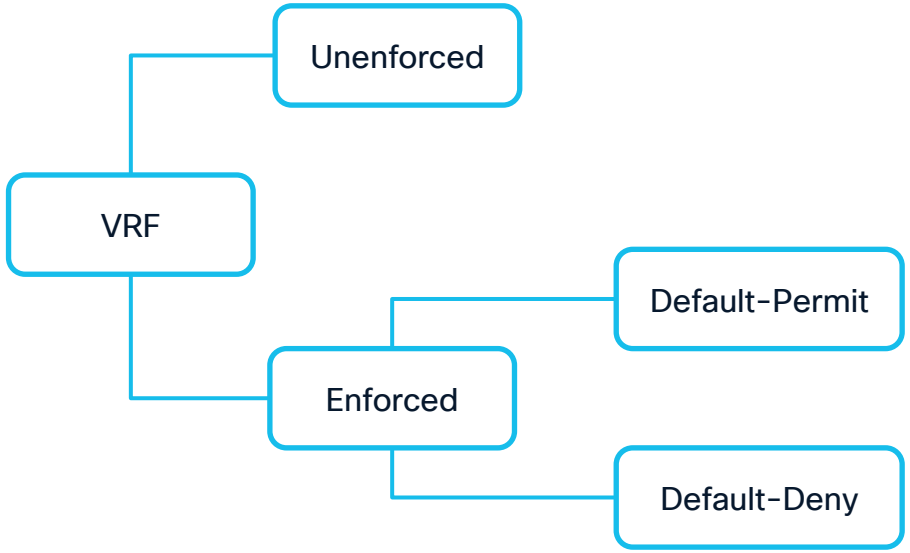



```
vrf context my_vrf
  security con sou 100 dest any policy MANAGEMENT bidir
  security con sou any dest 500 policy BACKUP bidir
  security con sou any dest any policy FIREWALL-REDIRECTION bidir
```

Group Policy Option Fundamentals

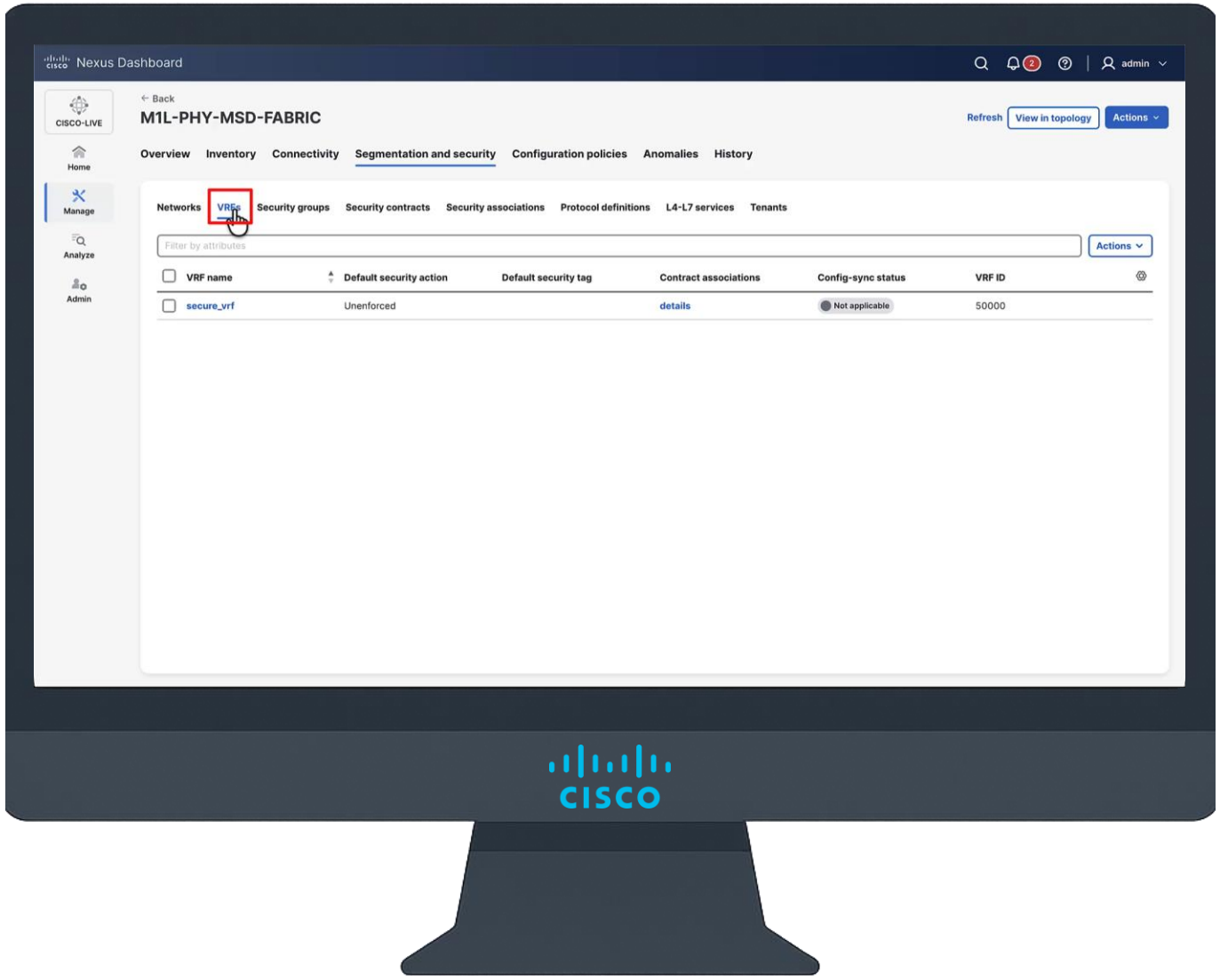
Traffic Enforcement – VRF Modes

- VRFs are the smallest atomic unit where traffic enforcement can be applied or denied
- They might be configured in 3 different options:
  - Unenforced: Classic behaviour, no policies
  - Enforced Permit: Block-List model, all traffic is allowed unless explicitly dropped
  - Enforced Deny: Allow-List model, all traffic is denied unless explicitly permitted
- Each VRF must be set with a default security tag for special classification, like BUM, multicast and for traffic that has not been categorized yet



Group Policy Option Fundamentals

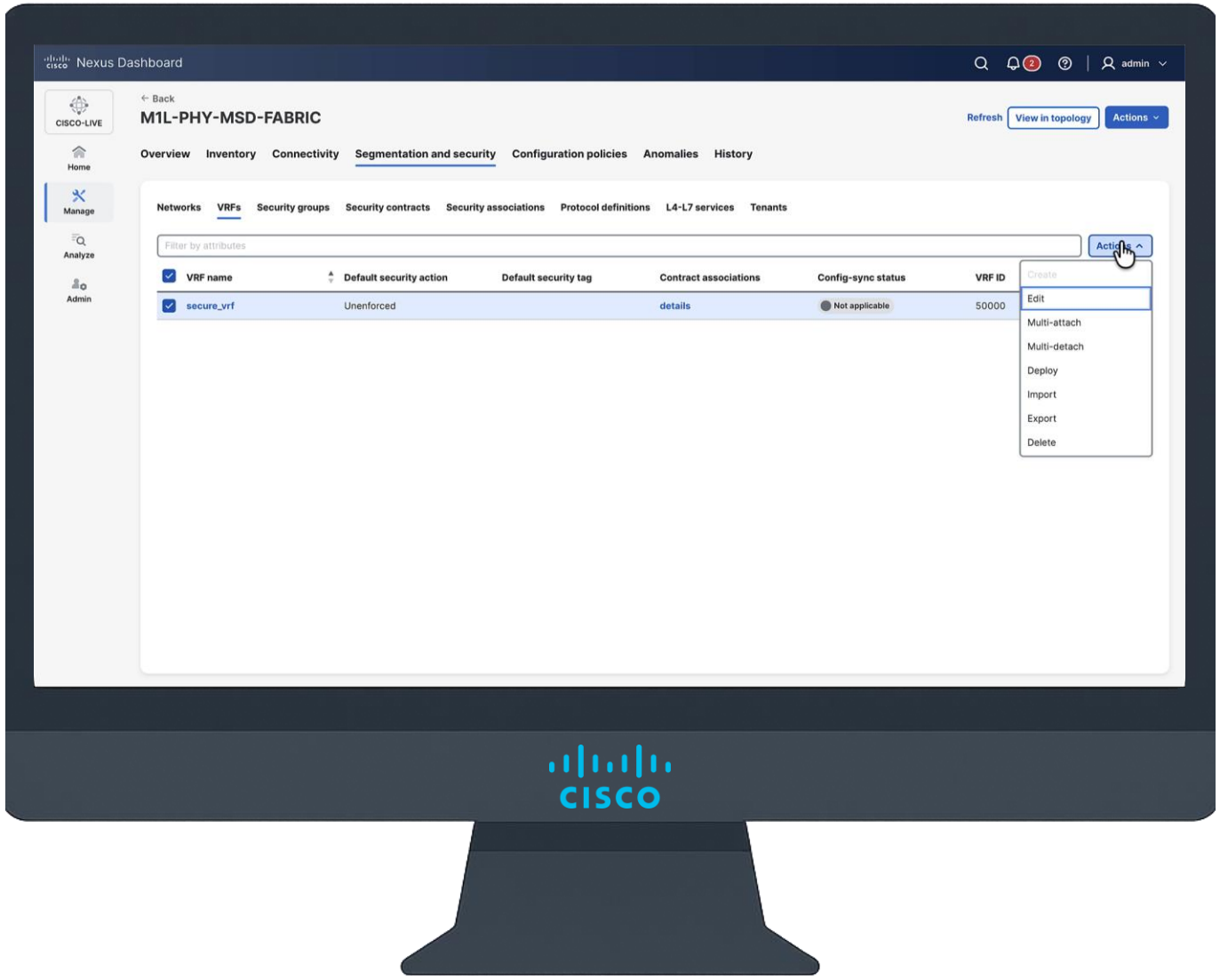
Nexus Dashboard – VRF Enforcement



cisco

Group Policy Option Fundamentals

Nexus Dashboard – VRF Enforcement

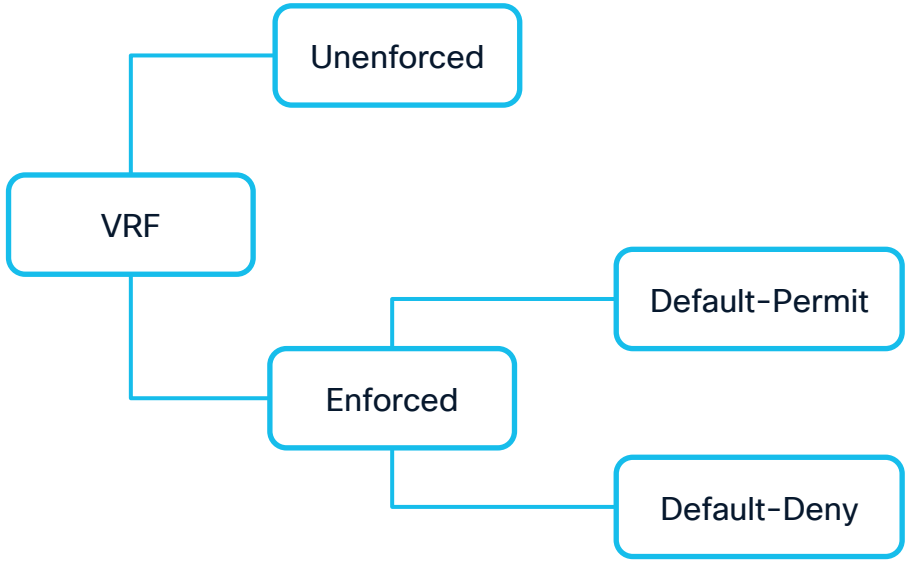


cisco

GPO Use Cases

Group Policy Option Fundamentals

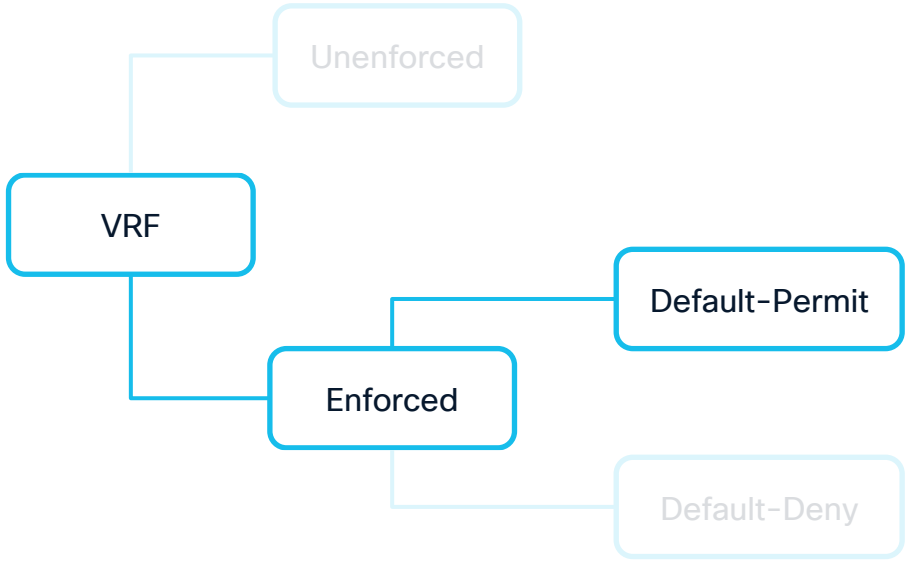
Traffic Enforcement



Group Policy Option Fundamentals

Traffic Enforcement – Enforced Permit

- Not very common, can be used when application traffic policy aren't fully documented and some flows must be dropped
- Legacy migration:
  - Minimal enforcement when moving endpoints from legacy
- Endpoint quarantine
  - Rapid containment of compromised hosts (e.g., zero-day response). Allows more control compared to RTBH
- Datacenter transit security
  - Block malicious, legacy, or reflection/amplification DDoS vectors between different customers/security-groups in transit VRFs



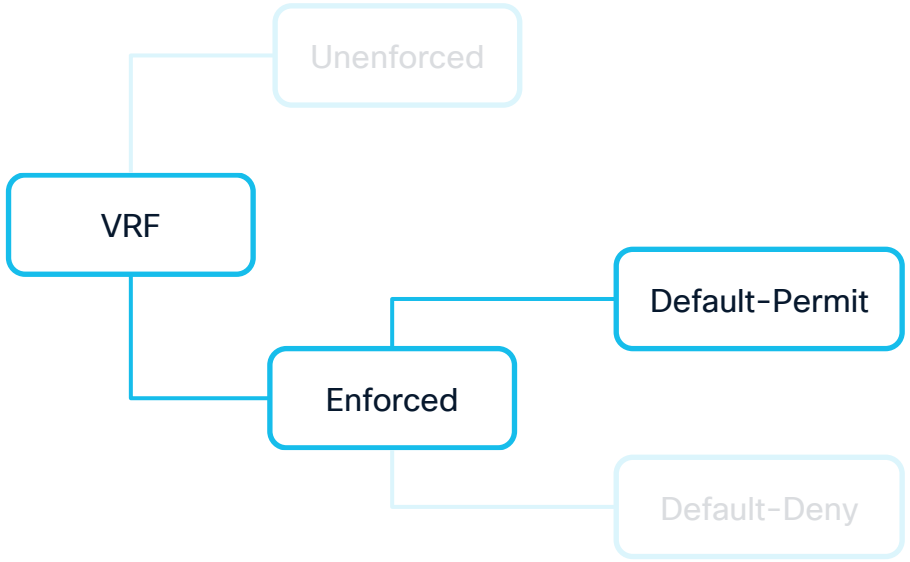

```
vrf context my_vrf
  security enforce tag 13129 default permit
```

Demo #1

Group Policy Option Fundamentals

Traffic Enforcement – Enforced Permit

- Not very common, can be used when application traffic policy aren't fully documented and some flows must be dropped
- Legacy migration:
  - Minimal enforcement when moving endpoints from legacy
- Endpoint quarantine
  - Rapid containment of compromised hosts (e.g., zero-day response). Allows more control compared to RTBH
- Datacenter transit security
  - Block malicious, legacy, or reflection/amplification DDoS vectors between different customers/security-groups in transit VRFs



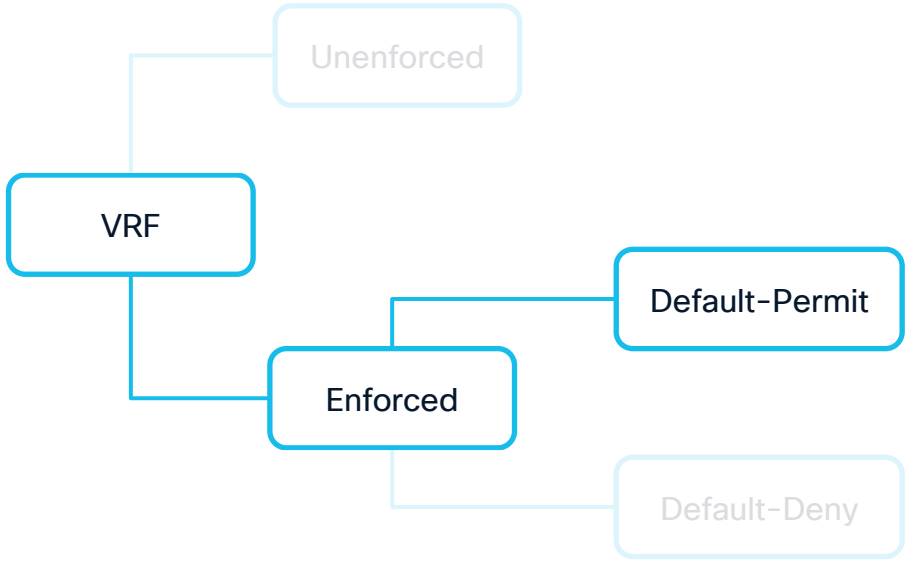

```
vrf context my_vrf
  security enforce tag 13129 default permit
```

Demo #2

Group Policy Option Fundamentals

Traffic Enforcement – Enforced Permit

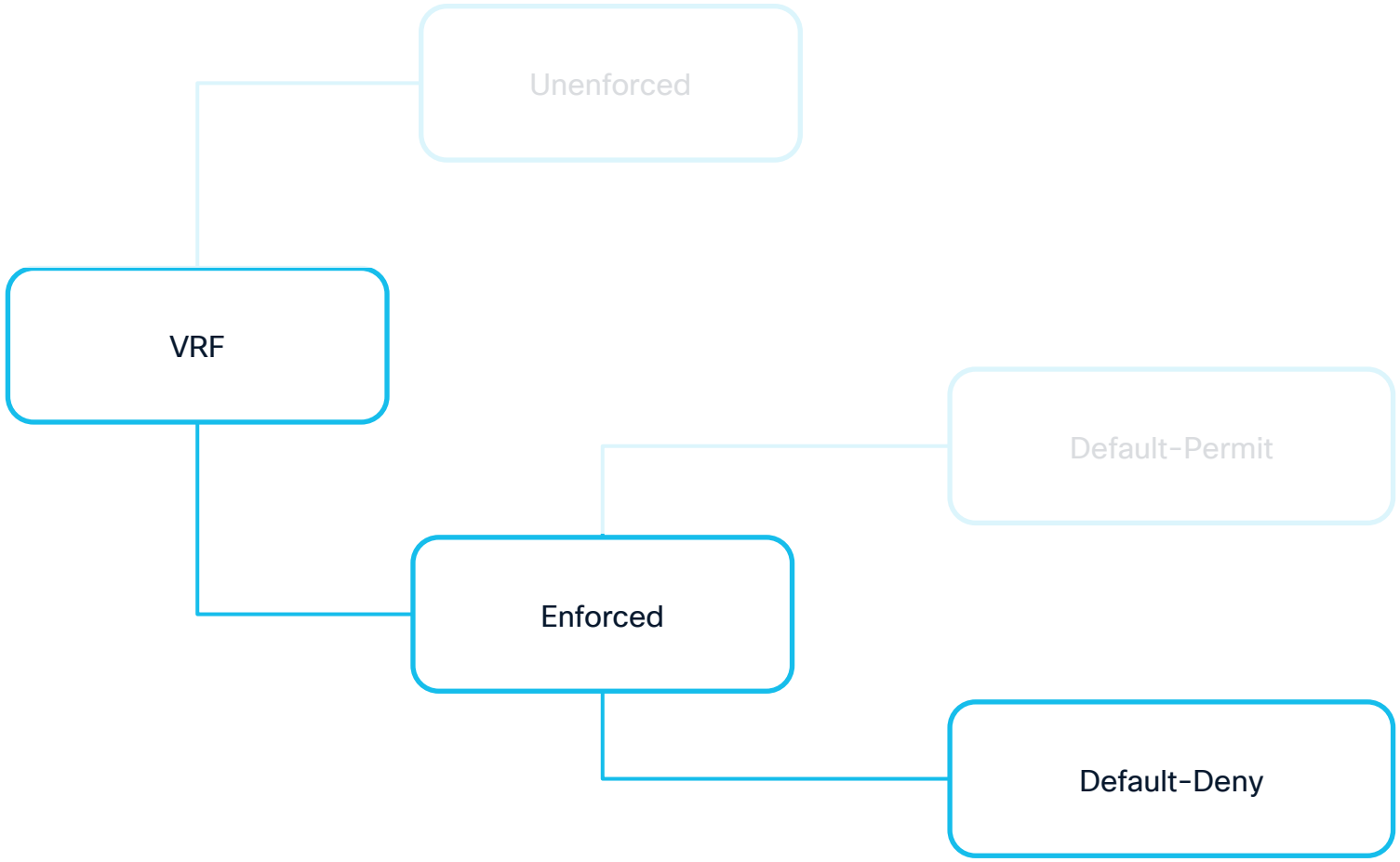
- Not very common, can be used when application traffic policy aren't fully documented and some flows must be dropped
- Legacy migration:
  - Minimal enforcement when moving endpoints from legacy
- Endpoint quarantine
  - Rapid containment of compromised hosts (e.g., zero-day response). Allows more control compared to RTBH
- Datacenter transit security
  - Block malicious, legacy, or reflection/amplification DDoS vectors between different customers/security-groups in transit VRFs




```
vrf context my_vrf
  security enforce tag 13129 default permit
```

Group Policy Option Fundamentals

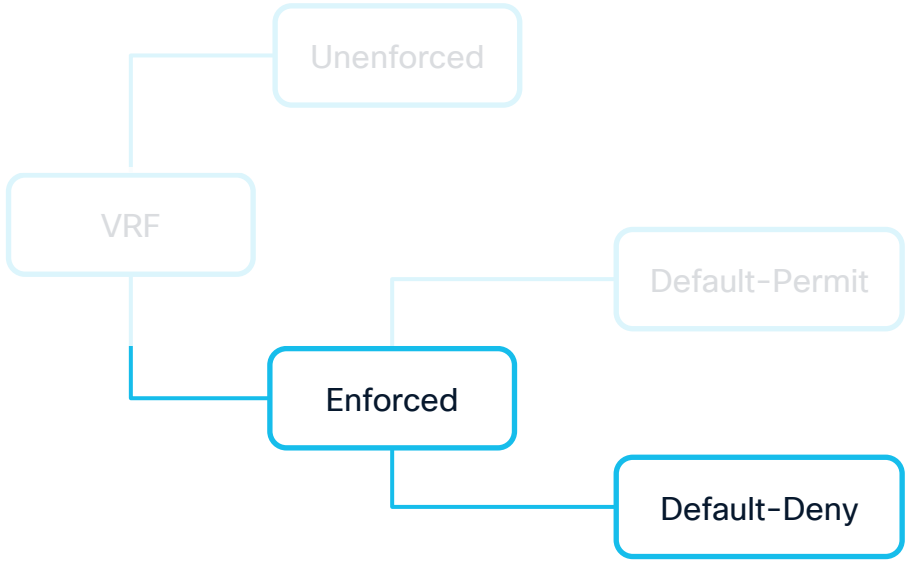
Traffic Enforcement – VRF Modes



Group Policy Option Fundamentals

Traffic Enforcement – Enforced Deny

- Real Zero-Trust model, multiple application levels
  - Subnet as Security Zone
    - Avoids the firewall as default-gateway
    - Reduces the VRFs
  - Application as Security Zone
    - Avoid proliferation of VRFs and networks
- Cloud-native approach
- Perfect for secured environments (PCI-DSS, HIPAA)



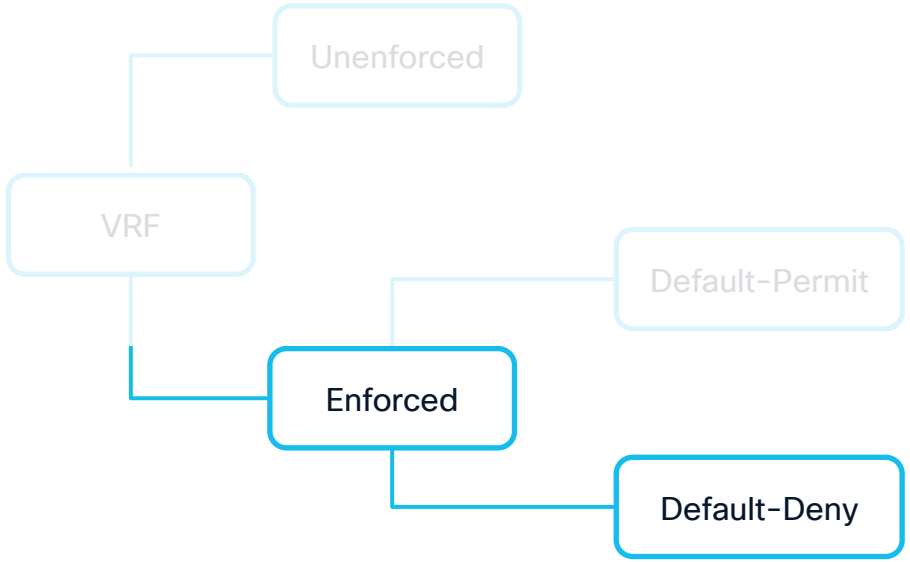

```
vrf context my_vrf
  security enforce tag 13129 default deny
```

Demo #3

Group Policy Option Fundamentals

Traffic Enforcement – Enforced Deny

- Real Zero-Trust model, multiple application levels
  - Subnet as Security Zone
    - Avoids the firewall as default-gateway
    - Reduces the VRFs
  - Application as Security Zone
    - Avoid proliferation of VRFs and networks
- Cloud-native approach
- Perfect for secured environments (PCI-DSS, HIPAA)



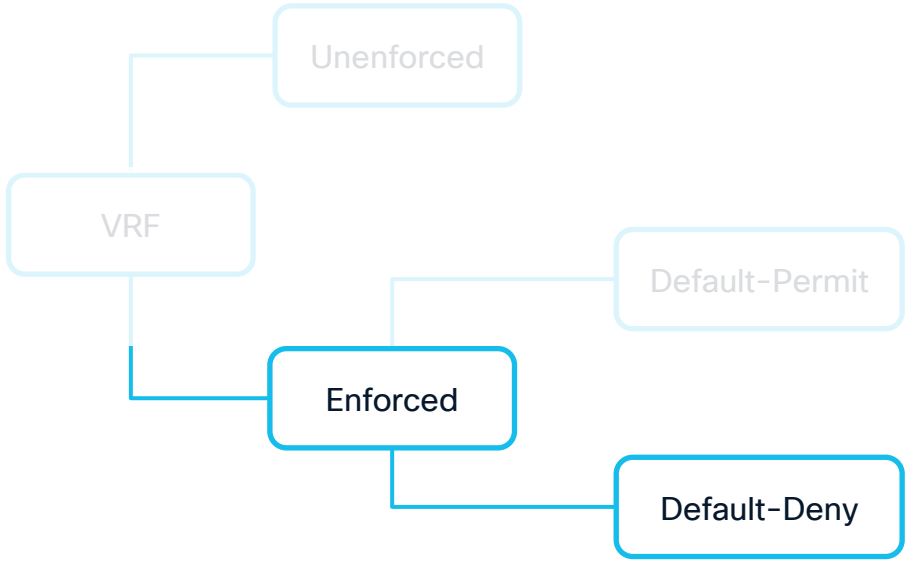

```
vrf context my_vrf
  security enforce tag 13129 default deny
```

Demo #4

Group Policy Option Fundamentals

Traffic Enforcement – Enforced Deny

- Real Zero-Trust model, multiple application levels
  - Subnet as Security Zone
    - Avoids the firewall as default-gateway
    - Reduces the VRFs
  - Application as Security Zone
    - Avoid proliferation of VRFs and networks
- Cloud-native approach
- Perfect for secured environments (PCI-DSS, HIPAA)




```
vrf context my_vrf
  security enforce tag 13129 default deny
```

Just because traffic is allowed doesn’t mean it’s innocent.

Security Team

GPO Based Service Redirection

Service Insertion

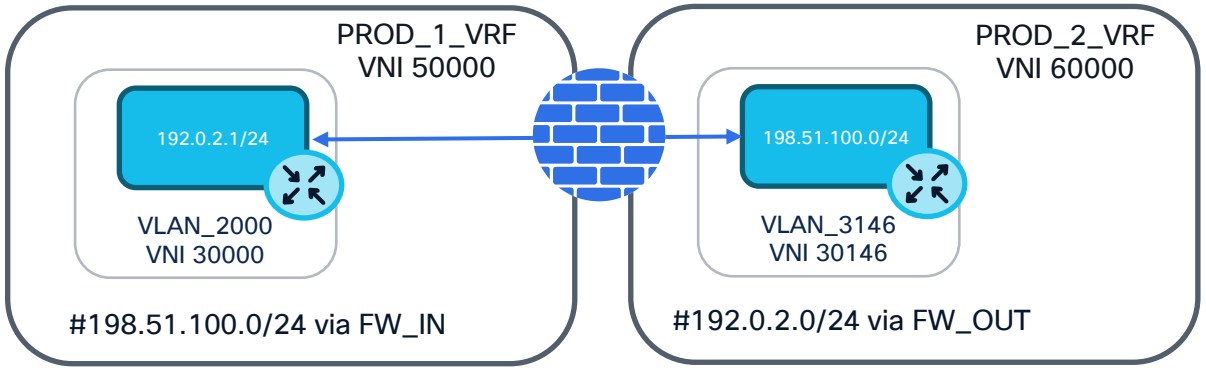
What is it and Why do we need it?

- Offload the traffic to a device connected to the fabric for additional processing
- Stateless ACLs might not be enough
- Companies' security policies might require advance traffic policies for some or all the traffic
- Security teams want to own the devices and the policies that inspect the traffic
- Redirection might also be used for other use cases:
  - NAT, CG-NAT
  - Load Balancing
  - TCP optimizers

Service Insertion

Classic Service Insertion Methods

- Classic methods require traffic to be forwarded to the firewall device by trusting the next hops present in the Layer-2 and Layer-3 RIBs/FIBs. IP/MAC lookup only
- Valid for many use cases:
  - Firewall As Default Gateway
  - Firewall As Perimeter Device
- Introduce configuration complexities and/or sub-optimal performances
- Administrators are forced to disable or work around key fabric functions.
  - DAG when firewall is used as default gateway
  - VRF Leaking with the perimeter firewall

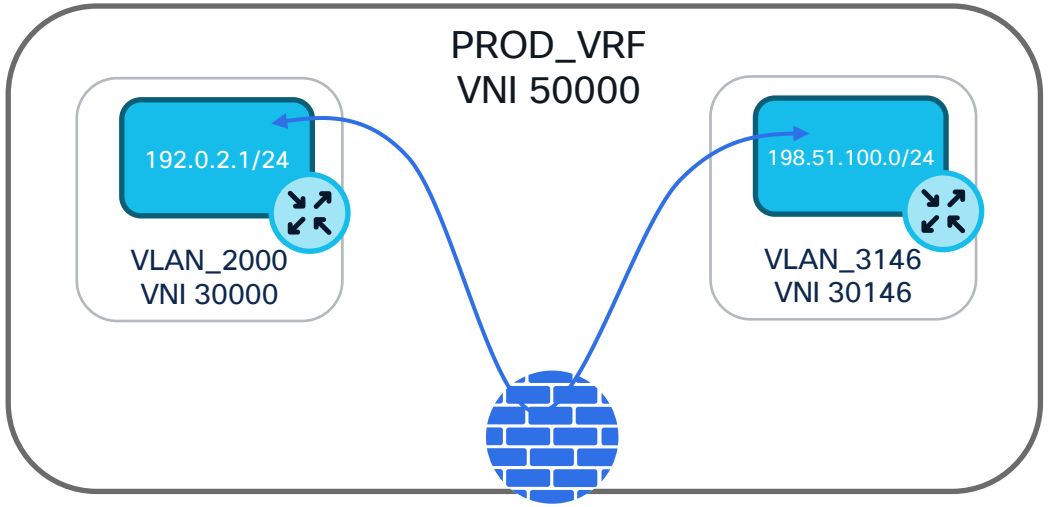


Classic VRF Sandwich

Service Insertion

Service Redirection Methods

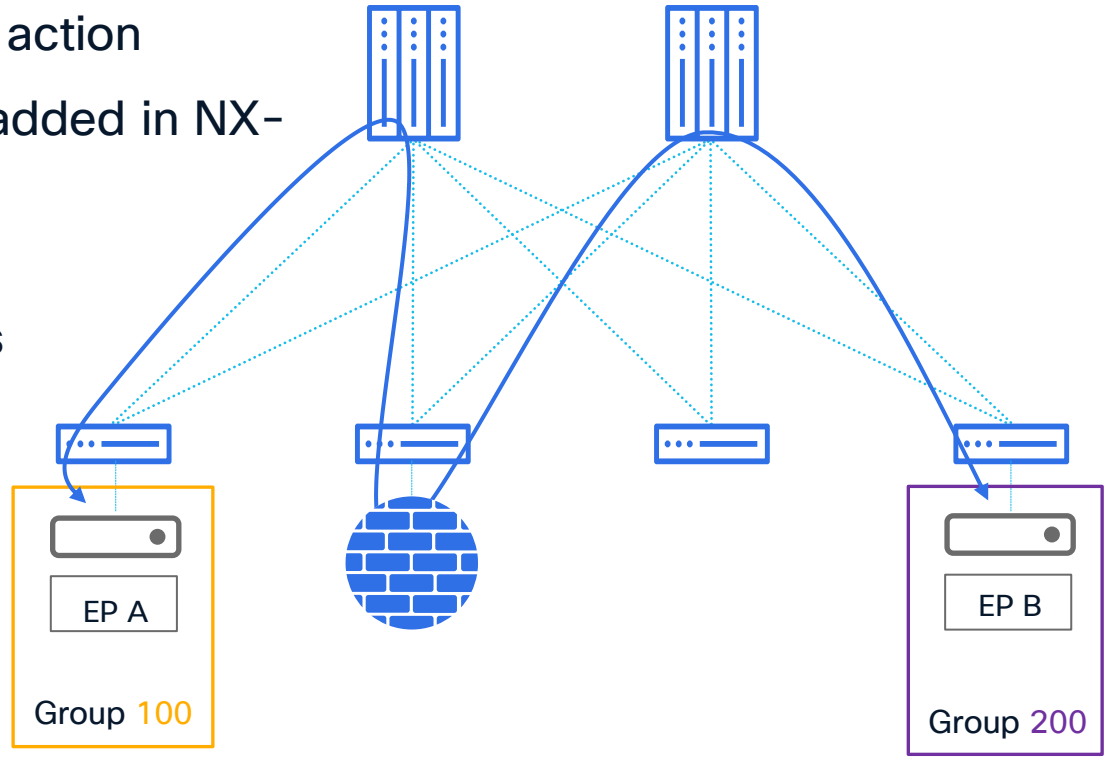
- Redirection/Stitching methods reroute traffic through security devices based on defined policies, there is no need to influence Layer-2 and Layer-3 RIBs/FIBs
- Redirection is totally decoupled from the topology
- NX-OS has multiple features that helps administrators under the ePBR umbrella term
  - Available since NX-OS 9.3(5)
  - Automated and simplified configuration
  - Ensures the symmetry will be maintained
  - Integrates monitoring and fail-action with IP SLA
  - Supports IP access-list and now GPO



GPO Based Service Redirection

Highlights

- GPO Service Redirection support introduced in NX-OS 10.5(1)F
- Extends SGACL capabilities with the service-chain action
- Multi-Site and multi-node Service Chains support added in NX-OS 10.5(2)F
  - Maximum 5 Service Functions
- Applicable for macro and micro segmentation rules
- Redirection can happen a subset of traffic
  - Granular match rules (filters)
- Not yet available in Nexus Dashboard
  - Workaround will be explored in the next demo

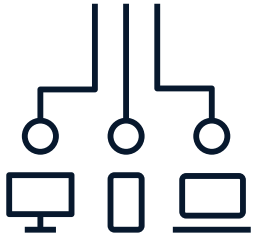


GPO Based Service Redirection

Terminology

Service Endpoint

This identifies the devices that will receive the traffic



Service Function

An entity that includes one or multiple Service Endpoints used for the same logical function

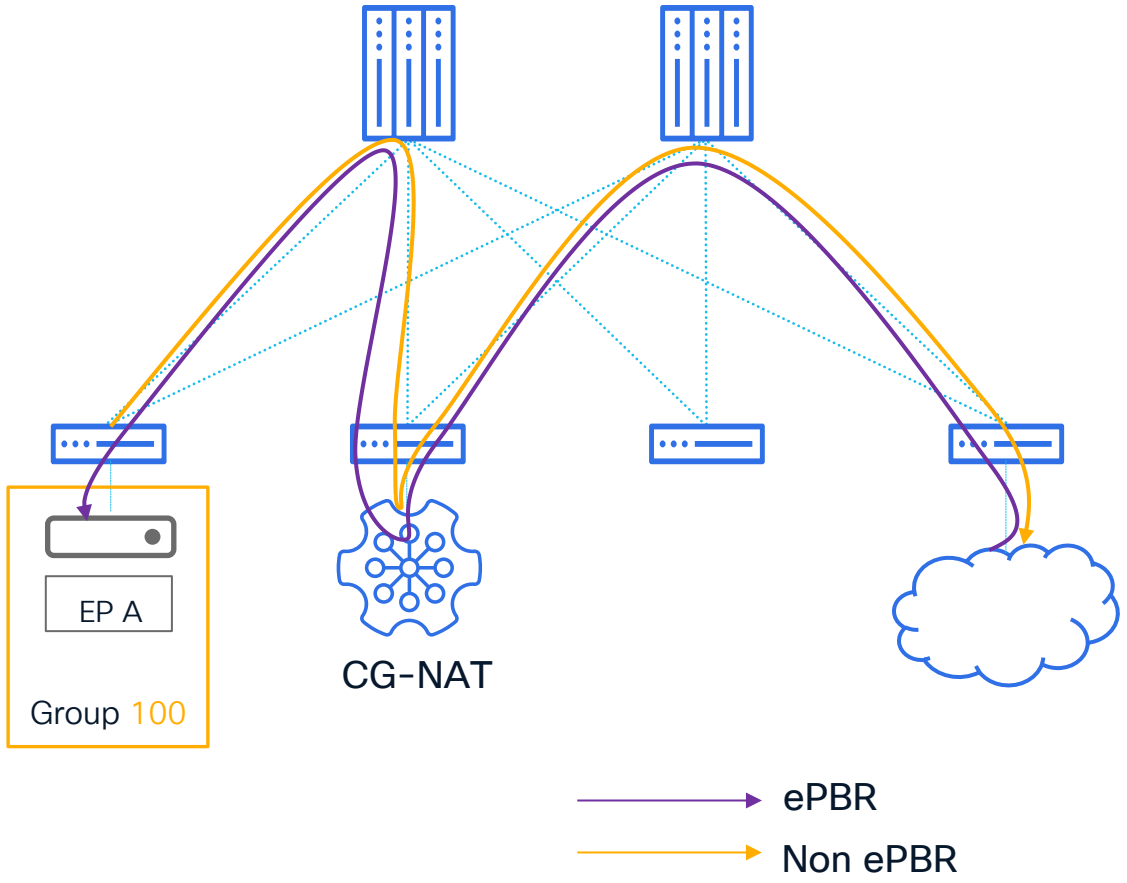
Service Chain

A list of one more Service Functions that Packets will need to traverse in the right order

GPO Based Service Redirection

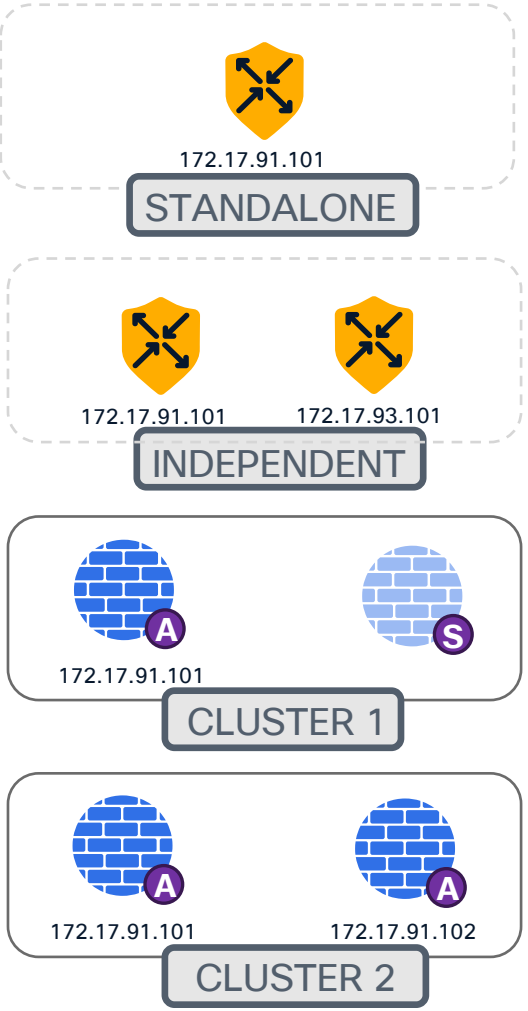
Service Endpoint

- Service Endpoints are networking devices that apply additional policies to the traffic
  - They must operate at Layer3
  - They can be Virtual or Physical
  - They can be standalone or deployed in clusters
- Depending on their function they might require different redirection rules
  - Device that do not apply any NAT rules like firewalls, IPS/IDS or TCP Optimizers
    - Redirection must be applied in both directions
  - Device that apply NAT rules like Load Balancers or CG-NAT devices
    - Redirection might be needed on one or both directions



GPO Based Service Redirection

Service Function

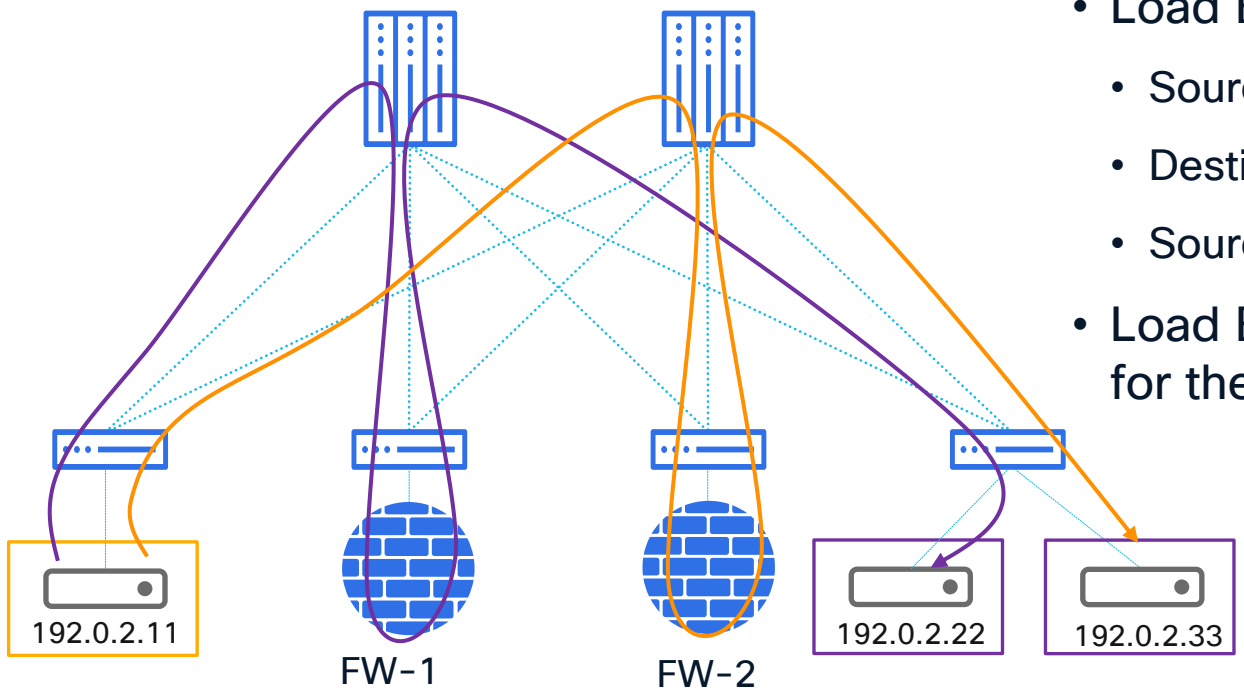


- Service Functions are logical groups of Service-Endpoints that enforce the same traffic policies.
- They can be used to set the IP SLA monitoring, and they will take the device in and out of the pool based on their status
- Can be associated to a single VRF
- When using GPO Service Functions returning traffic must be classified in a SG

```
security-group 10091 name FIREWALL-1
  type layer4-7
  match interface vlan 3101
epbr service FIREWALL-1-SITE-1
  vrf hyper_vrf
  security-group 10091
  probe icmp timeout 1 source-interface loopback98 frequency 2...
  service-end-point ip 172.17.91.101
  service-end-point ip 172.17.93.101
```

GPO Based Service Redirection

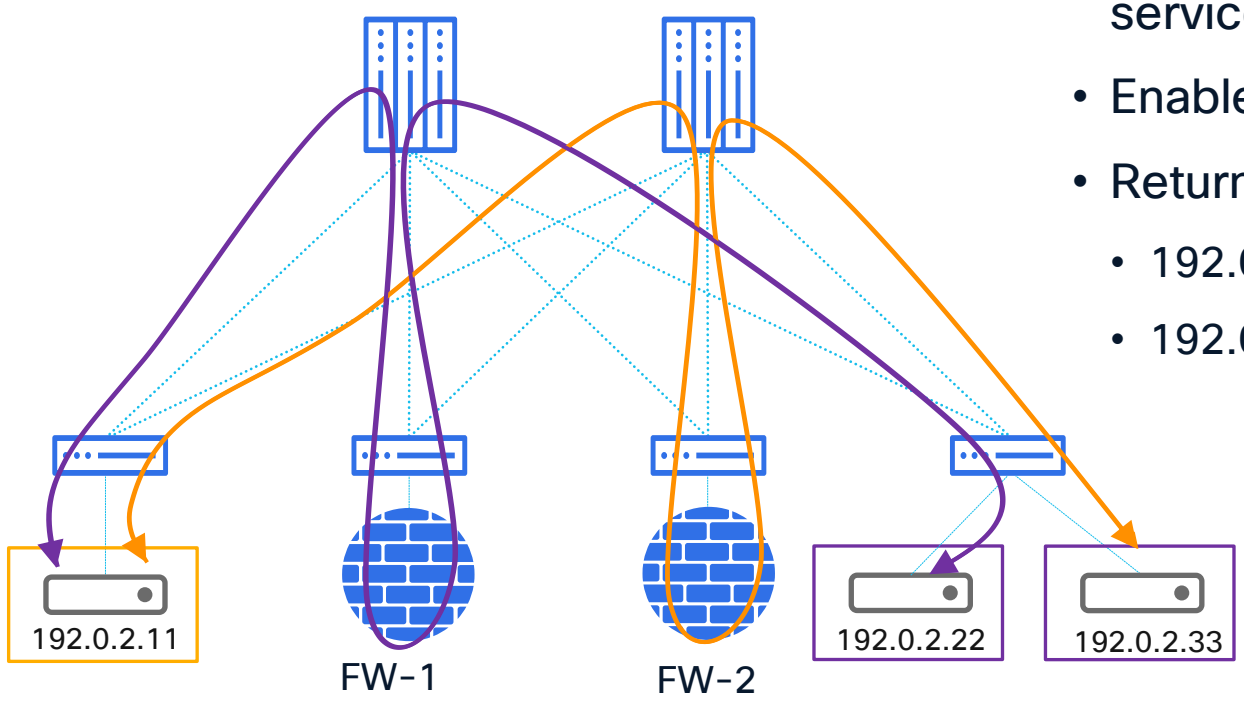
Load Balancing



- When a function has multiple endpoints with different IP addressed
- Load Balancing hash might be calculated based on:
  - Source IP Address
  - Destination IP Address
  - Source, Destination IP Addresses and IP Protocol
- Load Balancing can be set for the entire Service Chain or for the Service Function

GPO Based Service Redirection

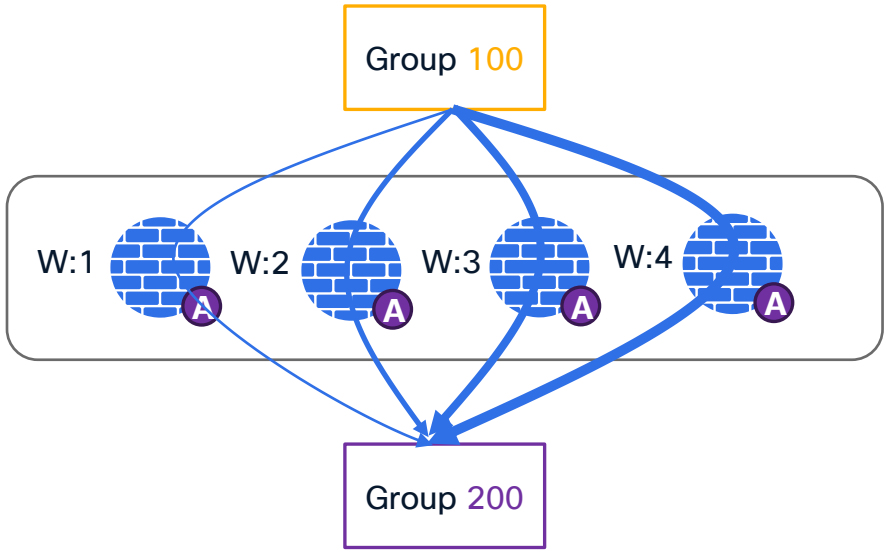
Load Balancing – Symmetric Hashing



- Load Balancing uses symmetric hashing
- Both flow directions will always be hashed in the same service endpoint
- Enabled by default
- Return traffic will always go to the same service endpoint
  - 192.0.2.11 -> 192.0.2.22 = FW-1 = 192.0.2.22 -> 192.0.2.11
  - 192.0.2.11 -> 192.0.2.33 = FW-2 = 192.0.2.33 -> 192.0.2.11

GPO Based Service Redirection

Load Balancing – Weighted Load Balancing

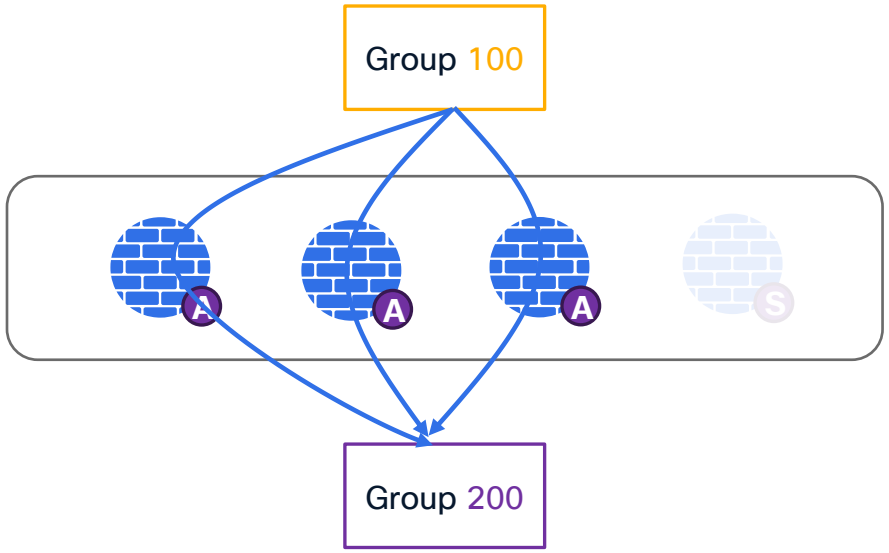


Assuming multiple IP addresses in both groups

- NX-OS can add two additional logics to hashing function:
- Weighted Load Balancing:
  - Unequally distributes the load over the different service endpoints
  - Allows different platforms with different scale/capacity in the same function
  - Smooths the impact of a policy change on a single (low weighted) device

GPO Based Service Redirection

Load Balancing – N+M Redundancy

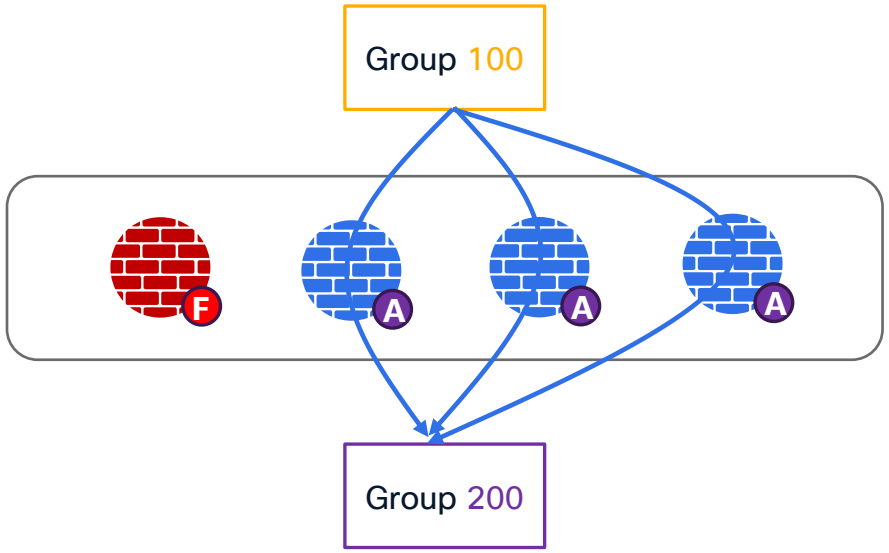


Assuming multiple IP addresses in both groups

- NX-OS can add two additional logics to hashing function:
- Weighted Load Balancing:
  - Unequally distributes the load over the different service endpoints
  - Allows different platforms with different scale/capacity in the same function
  - Smooths the impact of a policy change on a single (low weighted) device
- N+M Redundancy:
  - N Active service endpoints, M hot-standby devices

GPO Based Service Redirection

Load Balancing – N+M Redundancy



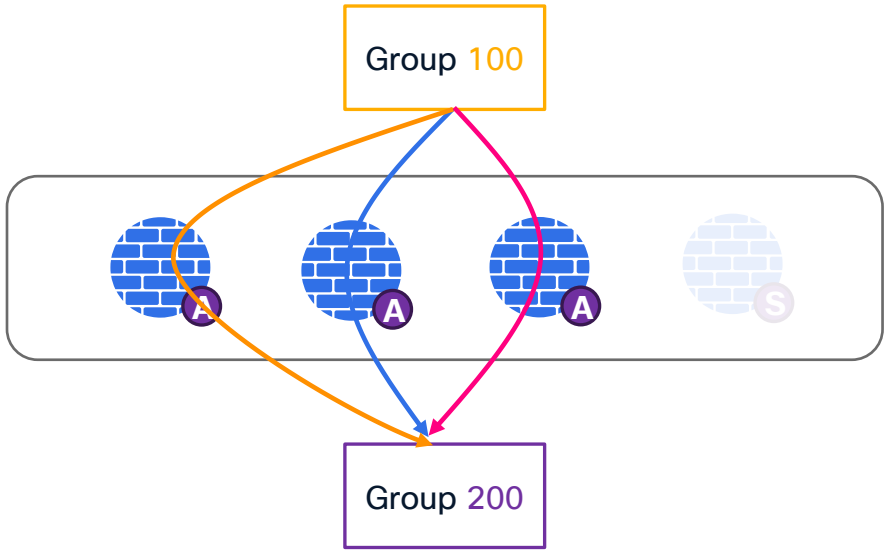
Assuming multiple IP addresses in both groups

- NX-OS can add two additional logics to hashing function:
- Weighted Load Balancing:
  - Unequally distributes the load over the different service endpoints
  - Allows different platforms with different scale/capacity in the same function
  - Smooths the impact of a policy change on a single (low weighted) device
- N+M Redundancy:
  - N Active service endpoints, M hot-standby devices
  - Standby will be promoted to active only on a N failure

GPO Based Service Redirection

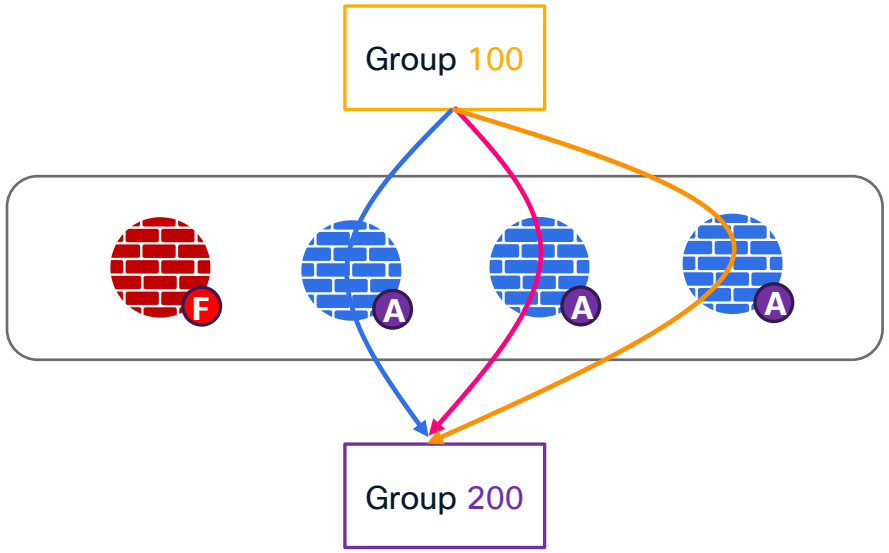
Load Balancing – Resilient Hashing

- Resilient Hashing drastically reduces the impact during failures inside of a redundant service chain



GPO Based Service Redirection

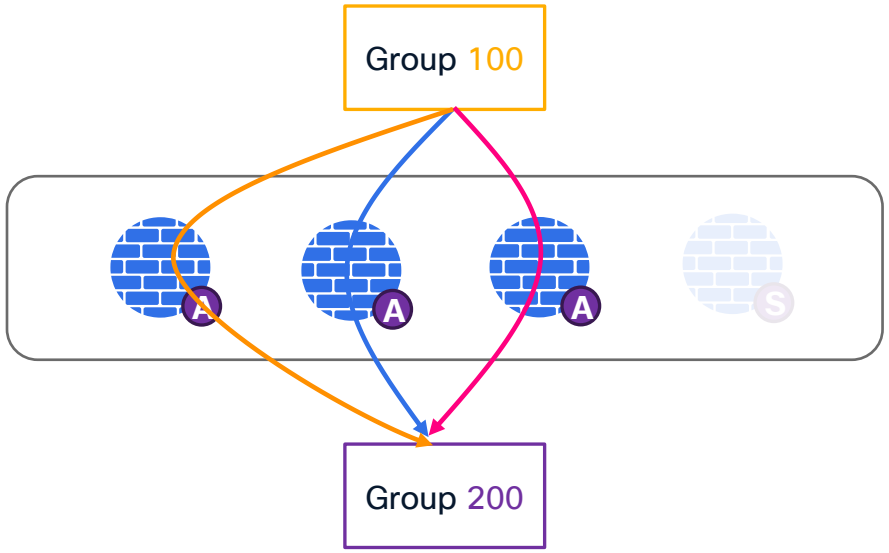
Load Balancing – Resilient Hashing



- Resilient Hashing drastically reduces the impact during failures inside of a redundant service chain
- When a service endpoint fails only the flows that were being hashed trough it will be re-hashed

GPO Based Service Redirection

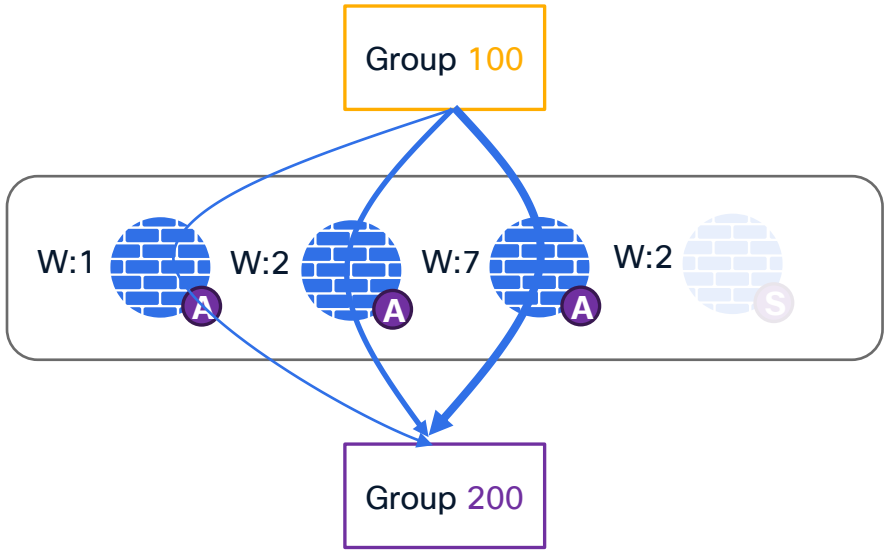
Load Balancing – Resilient Hashing



- Resilient Hashing drastically reduces the impact during failures inside of a redundant service chain
- When a service endpoint fails only the flows that were being hashed trough it will be re-hashed
- When a failed service endpoint becomes available again then only the original flows that were sent there will be re impacted
- Only works when active devices fail and get back active.

GPO Based Service Redirection

Load Balancing – Combining WLB and N+M

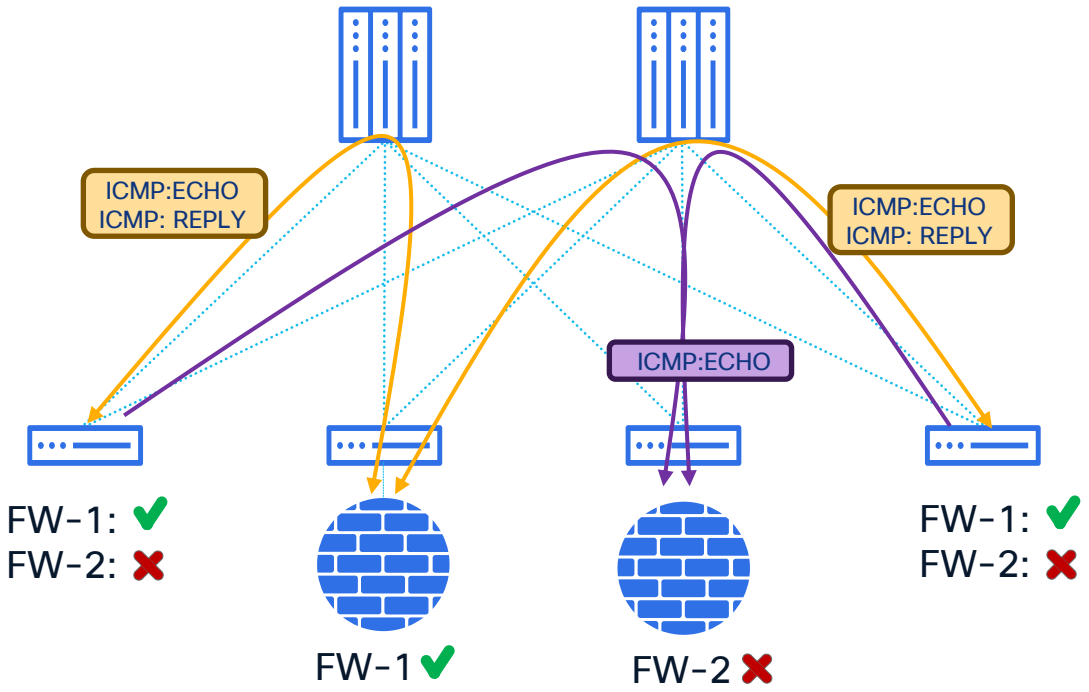


Assuming multiple IP addresses in both groups

- NX-OS can add two additional logics to hashing function:
- Weighted Load Balancing:
  - Unequally distributes the load over the different service endpoints
  - Allows different platforms with different scale/capacity in the same function
  - Smooths the impact of a policy change on a single (low weighted) device
- N+M Redundancy:
  - N Active service endpoints, M hot-standby devices
  - Standby will be marked as active only on N failure
- Both can be combined:
  - M endpoints will only replace a N node with same or lower weight

GPO Based Service Redirection

Service Function - Tracking

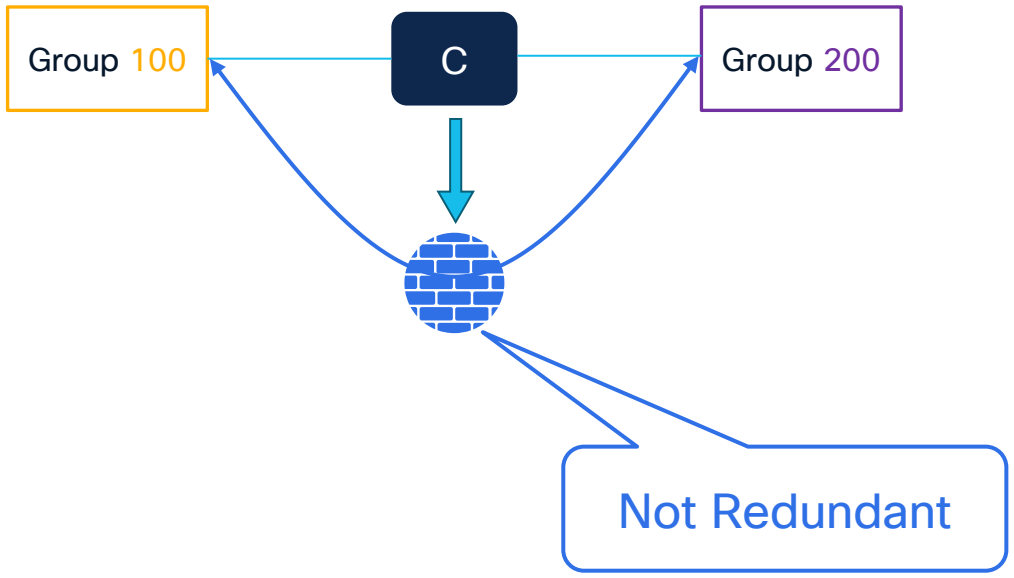


- Tracking the health of devices avoids blackholes
- All the VTEPs where the traffic is forwarded needs to track the status of the devices via loopbacks
- Unhealthy Service Endpoints must be excluded from the Service Function pool
- Probes can be configured with different protocols
  - ICMP
  - UDP
  - TCP
  - HTTP
- Probes must be sourced from a Loopback, you cannot use a DAG SVI

GPO Based Service Redirection

Service Chains - Single Function

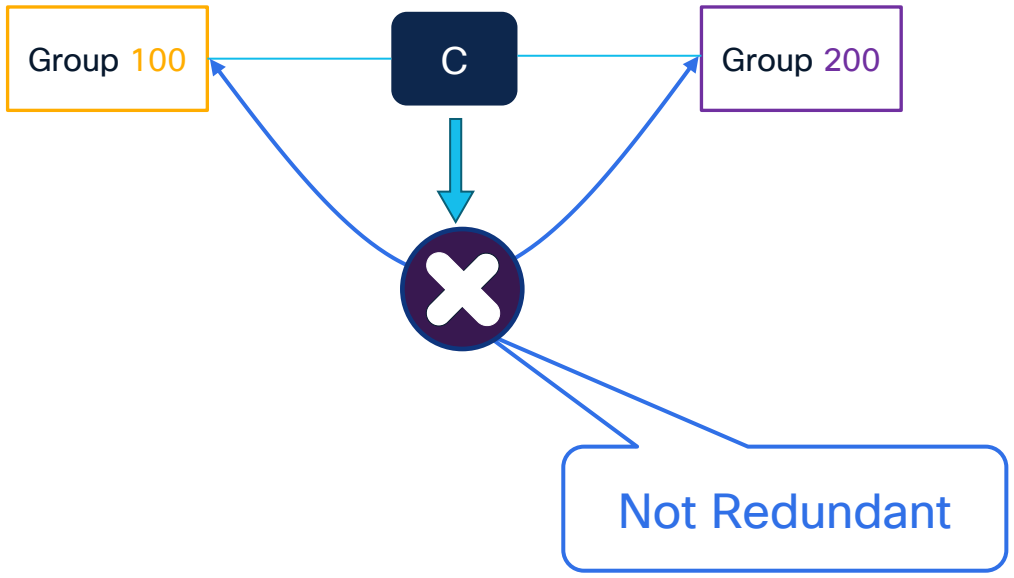
- Service Chains allow us to define the traffic redirection rules.
- When traffic is redirected to a service-chain it needs to cross all the functions listed there.




```
epbr service-chain WEB-CHAIN-SITE-1
  load-balance method src-dst-ipprotocol
 10 set service FIREWALL-1-SITE-1
  action redirect
```

GPO Based Service Redirection

Service Chains – Single Function

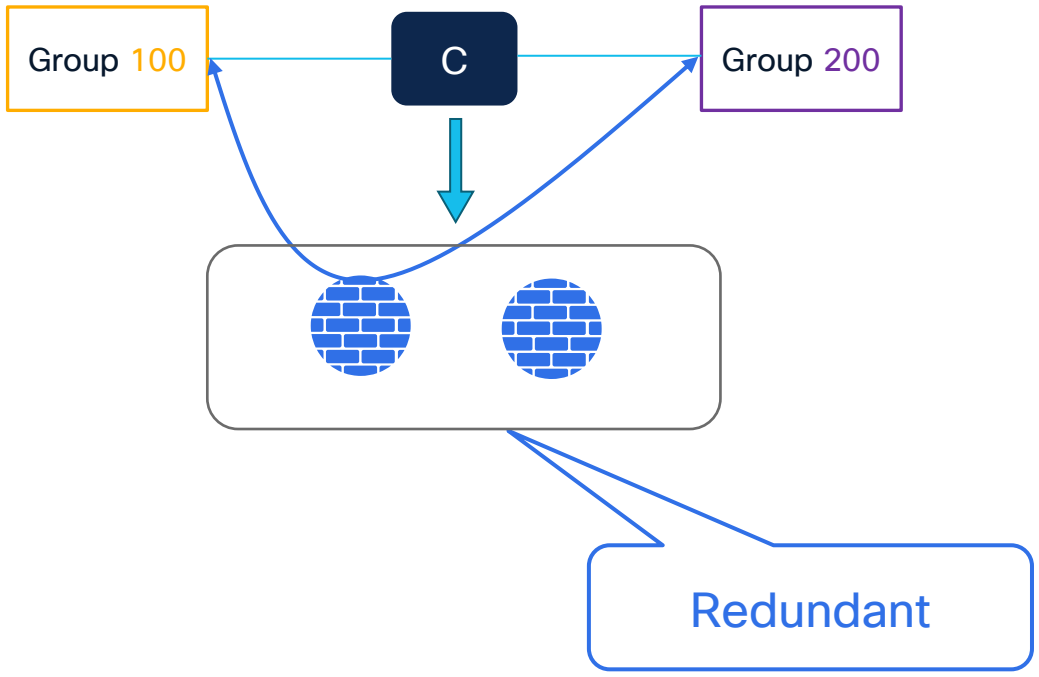


- Service Chains allow us to define the traffic redirection rules.
- When traffic is redirected to a service-chain it needs to cross all the functions listed there.
  - If a function is not UP, we can decide the action
    - Forward – Send the packet to the destination IP
    - Drop – Discard the packet
    - ~~Bypass~~ (not useful with single function service-chains)
- Single Function Service Chains have one step only

```
epbr service-chain WEB-CHAIN-SITE-1
  load-balance method src-dst-ipprotocol
  10 set service FIREWALL-1-SITE-1 fail-action drop
   action redirect
```

GPO Based Service Redirection

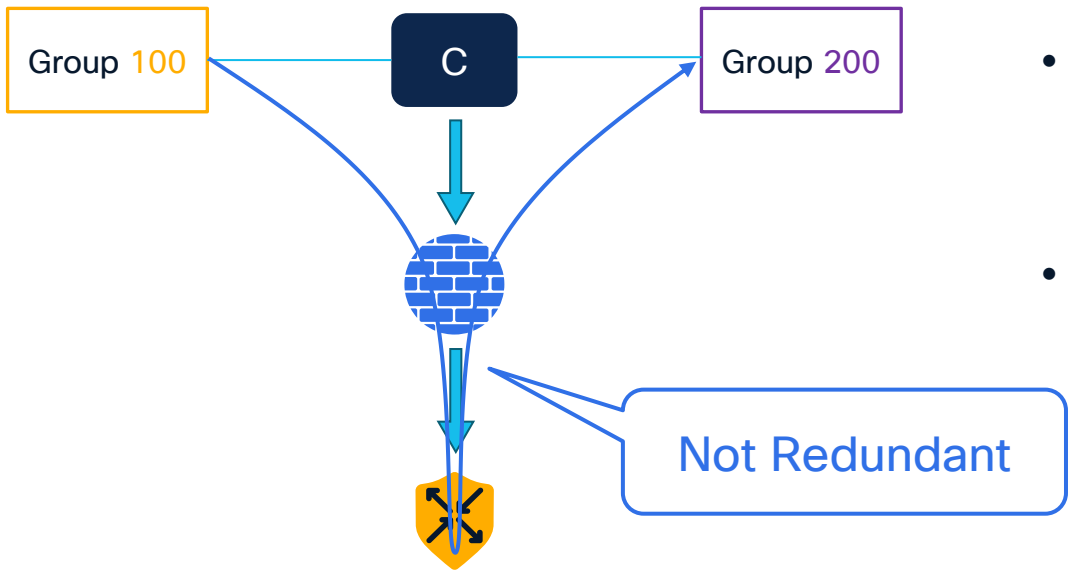
Service Chains - Single Function



- Redundancy can be obtained in different ways
  - Cluster: Active/Standby or Active/Active
  - Independent devices with synchronized policies
- Symmetry is always maintained
  - When multiple service endpoints, with different IP addresses, are defined inside a function, traffic in both directions is always sent to the same node

GPO Based Service Redirection

Service Chains – Multi Function

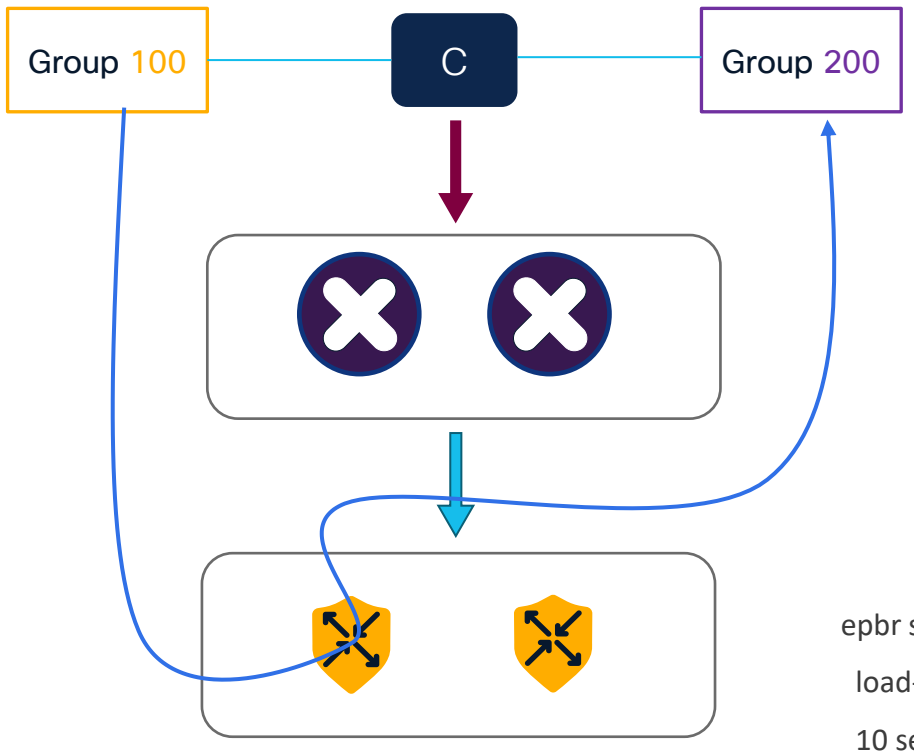


- Service Chains can contain multiple functions
- Each function is mapped to a sequence number that sets the order
  - Returning traffic will follow the order backwords
- If a function is not UP, we can decide the action
  - ~~Forward~~ – (cannot be used with multi function service-chains)
  - Drop – Discard the packet
  - Bypass – Redirect to the next function

```
epbr service-chain WEB-CHAIN-SITE-1
  load-balance method src-dst-ipprotocol
  10 set service FIREWALL-1-SITE-1 fail-action bypass
    action redirect
  20 set service IDS-1-SITE-1 fail-action drop
    action redirect
```

GPO Based Service Redirection

Service Chains – Multi Function



- Service Chains can contain multiple functions
- Each function is mapped to a sequence number that sets the order
  - Returning traffic will follow the order backwords
- If a function is not UP, we can decide the action
  - ~~Forward~~ – (cannot be used with multi function service-chains)
  - Drop – Discard the packet
  - Bypass – Redirect to the next function

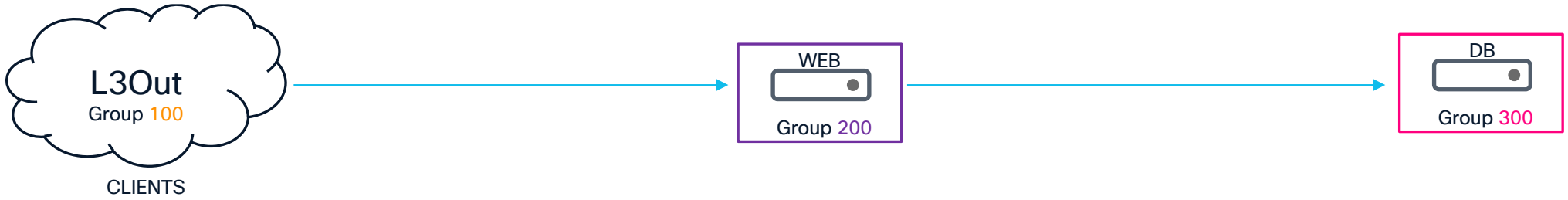
```
epbr service-chain WEB-CHAIN-SITE-1
  load-balance method src-dst-ipprotocol
  10 set service FIREWALL-1-SITE-1 fail-action bypass
    action redirect
  20 set service IDS-1-SITE-1 fail-action drop
    action redirect
```

GPO Based Service Redirection

Enhanced Evergreen Example

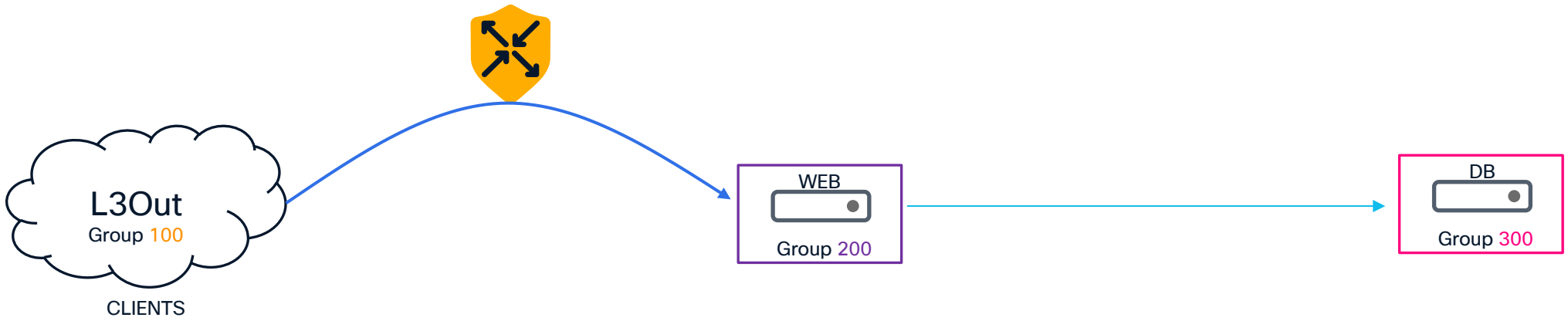
```
security-group 200 name WEB-CLIENT
  match external-subnets vrf hyper_vrf ipv4 203.0.113.128/25 route-inject

security-group 200 name WEB
  match connected-endpoints vrf hyper_vrf ipv4 198.51.100.10/32
  match connected-endpoints vrf hyper_vrf ipv4 198.51.100.15/32

security-group 300 name WEB
  match connected-endpoints vrf hyper_vrf ipv4 198.51.100.201/32

vrf context hyper_vrf
   security enforce tag 13129 default deny
   security contract source 100 destination 200 policy TO-WEB
   security contract source 200 destination 300 policy TO-DB
```

```
class-map type security match-any WEB-PORTS
  match ipv4 tcp stateful dport 443
  match ipv4 tcp stateful dport 80
class-map type security match-any DB-PORTS
  match ipv4 tcp stateful dport 3306

policy-map type security TO-WEB
  class WEB-PORTS
    permit
policy-map type security TO-DB
  class DB-PORTS
    permit
```



GPO Based Service Redirection

Enhanced Evergreen Example

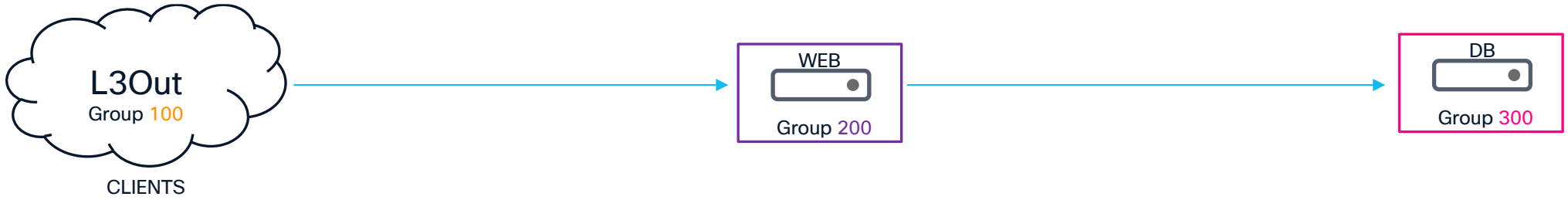


GPO Based Service Redirection

Enhanced Evergreen Example – Configurations That Will Not Change

```
security-group 200 name WEB-CLIENT
  match external-subnets vrf hyper_vrf ipv4 203.0.113.128/25 route-inject

security-group 200 name WEB
  match connected-endpoints vrf hyper_vrf ipv4 198.51.100.10/32
  match connected-endpoints vrf hyper_vrf ipv4 198.51.100.15/32

security-group 300 name WEB
  match connected-endpoints vrf hyper_vrf ipv4 198.51.100.201/32

vrf context hyper_vrf
  security enforce tag 13129 default deny
  security contract source 100 destination 200 policy TO-WEB
  security contract source 200 destination 300 policy TO-DB
```

```
class-map type security match-any WEB-PORTS
  match ipv4 tcp stateful dport 443
  match ipv4 tcp stateful dport 80
class-map type security match-any DB-PORTS
  match ipv4 tcp stateful dport 3306

policy-map type security TO-WEB
  class WEB-PORTS
    permit
policy-map type security TO-DB
  class DB-PORTS
    permit
```

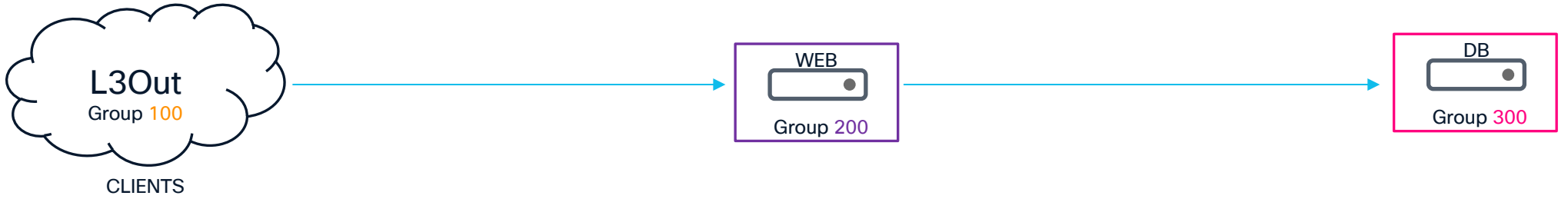


GPO Based Service Redirection

Enhanced Evergreen Example – Service Definition

```
security-group 10091 name WAF-1
  type layer4-7
  match interface vlan 3101
epbr service WAF
  vrf hyper_vrf
  security-group 10091
  probe icmp timeout 1 source-interface lo98
  service-end-point ip 172.17.91.101
    service-end-point ip 172.17.91.102
epbr service-chain SERVICE-CHAIN-WAF
  10 set service WAF
    action redirect
```

```
policy-map type security TO-WEB
  class WEB-PORTS
    permit
```



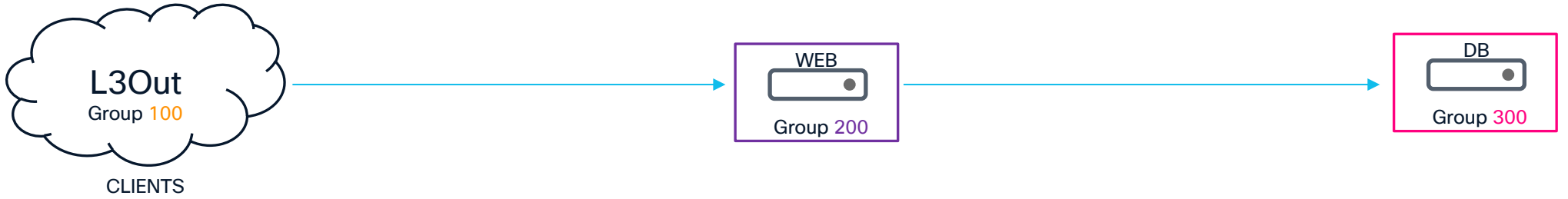
cisco

GPO Based Service Redirection

Enhanced Evergreen Example – Service Association

```
security-group 10091 name WAF-1
  type layer4-7
  match interface vlan 3101
epbr service WAF
  vrf hyper_vrf
  security-group 10091
  probe icmp timeout 1 source-interface lo98
  service-end-point ip 172.17.91.101
    service-end-point ip 172.17.91.102
epbr service-chain SERVICE-CHAIN-WAF
  10 set service WAF
    action redirect
```

```
policy-map type security TO-WEB
  class WEB-PORTS
    service-chain SERVICE-CHAIN-WAF
```



cisco

Demo#5

Conclusions

Summary

New Security Options for VXLAN EVPN Fabrics

- We just discovered new functionalities that can greatly enhance the security in your Data Center networks
- Group Policy Option:
  - With dynamic classification and grouping of connected endpoints and external networks
  - Remediates persistent security gaps in legacy, migrated environments
  - Essential for new secure greenfield deployments
- Service Redirection with GPO:
  - Easily design and configure the integration between GPO and ePBR service redirection
  - Flexibly map the flows that need to be sent to external devices for additional policies
- Available on standalone NX-OS and Nexus Dashboard*
  - Automation can be achieved with both operational models
  - Automation can integrate external data sources and/or logics

*GPO Service Redirection workflows: future

Resources

Continue your GPO journey

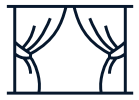
- NX-OS Group Policy Option White Paper:
  - https://www.cisco.com/c/en/us/td/docs/dcn/whitepapers/securing-datacenters-with-microsegmentation-and-vxlan-gpo.html
- NX-OS Group Policy Option Admin Guide:
  - https://www.cisco.com/c/en/us/td/docs/dcn/nx-os/nexus9000/106x/configuration/vxlan/cisco-nexus-9000-series-nx-os-vxlan-configuration-guide-release-106x/microsegmentation_for_vxlan_fabrics_using_gpo.html
- NX-OS Configuring Service Chaining with Security Groups:
  - https://www.cisco.com/c/en/us/td/docs/dcn/nx-os/nexus9000/106x/configuration/epbr/cisco-nexus-9000-series-nx-os-epbr-configuration-guide/chapter.html

Complete your session surveys

Complete your surveys in the Cisco Events App.

Complete a minimum of 4 session surveys and the overall event survey to receive a unique Cisco Live t-shirt.
(from 11:30 on Thursday, while supplies last)

Continue your education



Visit the Cisco Showcase for related demos

Book your one-on-one Meet the Engineer meeting

Visit the Technical Solutions Clinics to discuss your technical questions

Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs

Visit the On-Demand Library for more sessions at CiscoLive.com/On-Demand

Thank you

cisco Live !


CISCO