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

Max Ardica
Distinguished TME

cisco Live !

Session ID: BRKDCN-2909

Cisco Webex App

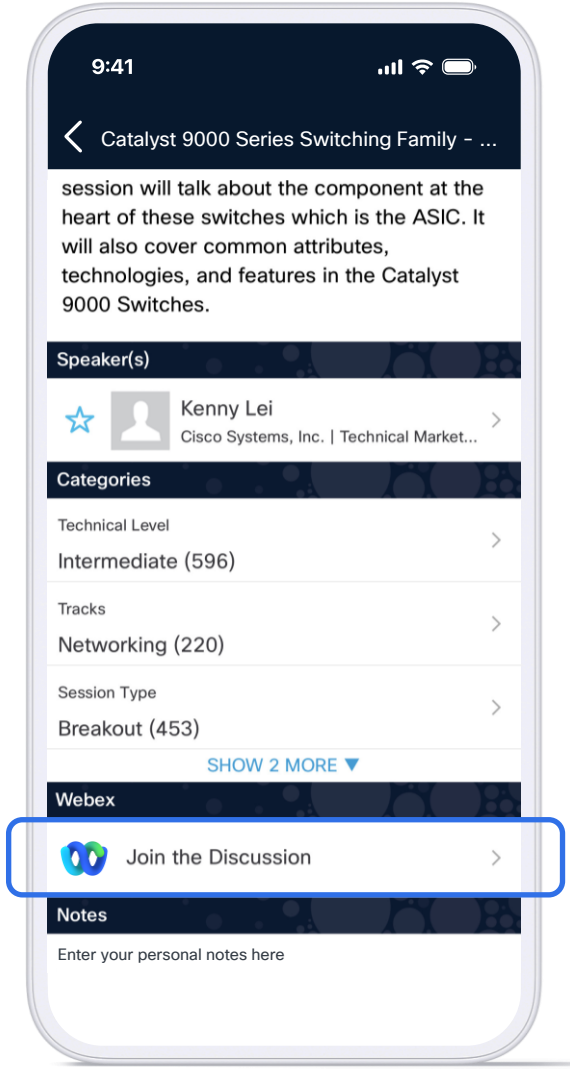
Questions?

Use Cisco Webex App to chat
with the speaker after the session

How

1. Find this session in the Cisco Live Mobile 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 14 November 2025.



https://ciscolive.ciscoevents.com/
ciscolivebot/**#BRKDCN-2909**

© 2025 Cisco and/or its affiliates. All rights reserved.

Agenda

01 Introduction

02 Group Policy Option Origin

03 Group Policy Option Fundamentals

04 GPO Based Service Redirection

© 2025 Cisco and/or its affiliates. All rights reserved.

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 (GPO)
  - Service Redirection based on GPO

© 2025 Cisco and/or its affiliates. All rights reserved.

Group Policy Option

Enhancing Data Center Segmentation with Simplicity and Granularity

GPO Standard

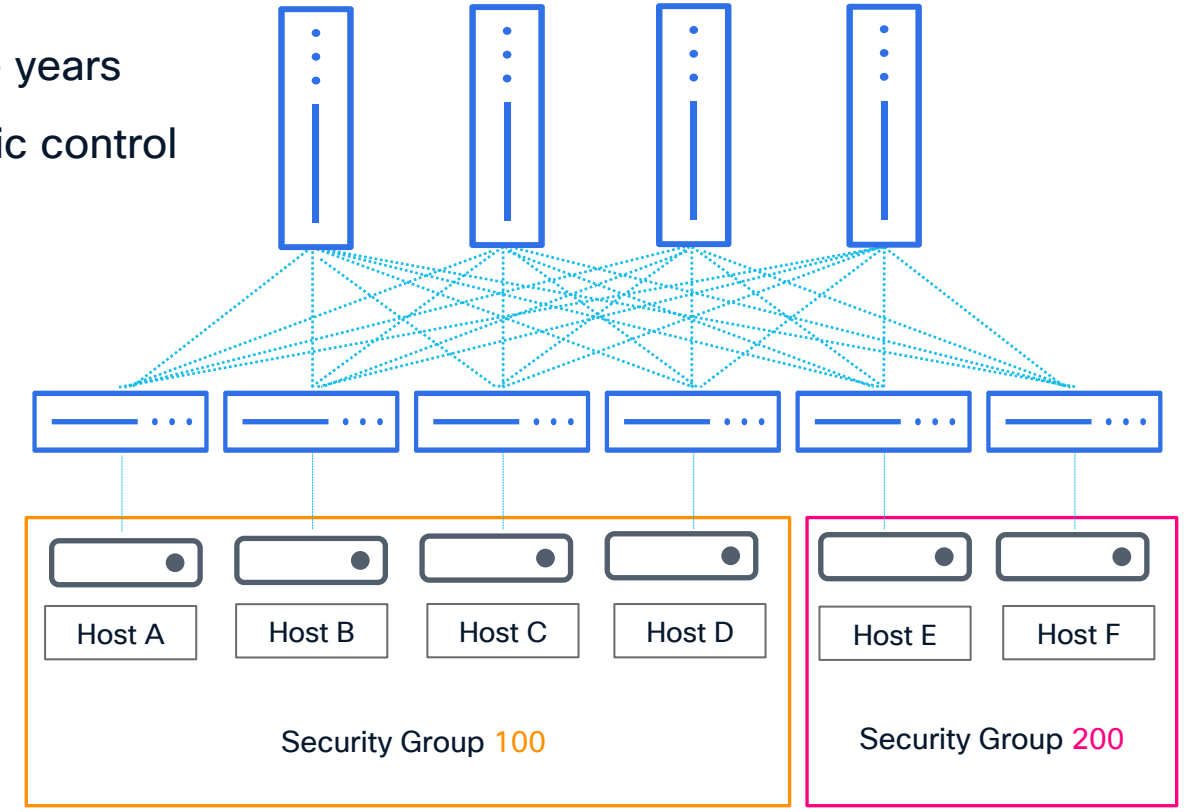
- First published in 2014, with many enhancements over the years
- Extension to VXLAN and EVPN that provide additional traffic control
- Backwards compatible

Grouping and Classification

- Classify endpoints into security-groups
- Based on IPs, MACs, VLANs and Ports

Enforcement for inter-group traffic

- Permit
- Deny
- Redirect



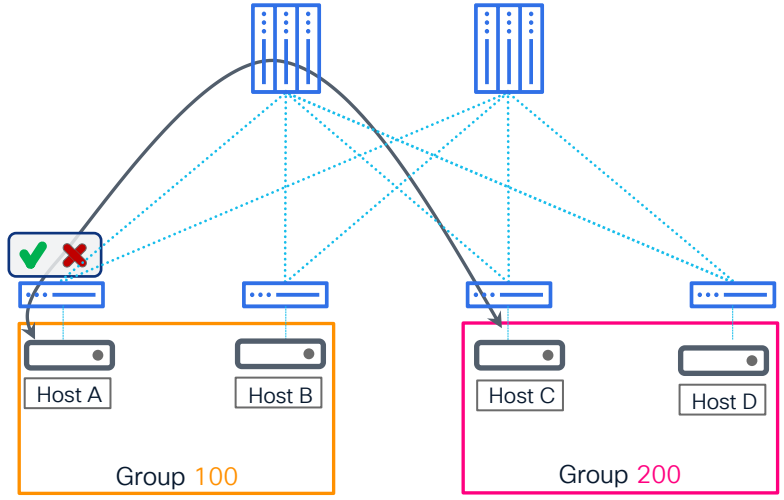
© 2025 Cisco and/or its affiliates. All rights reserved.

Group Policy Option

Main Use Cases

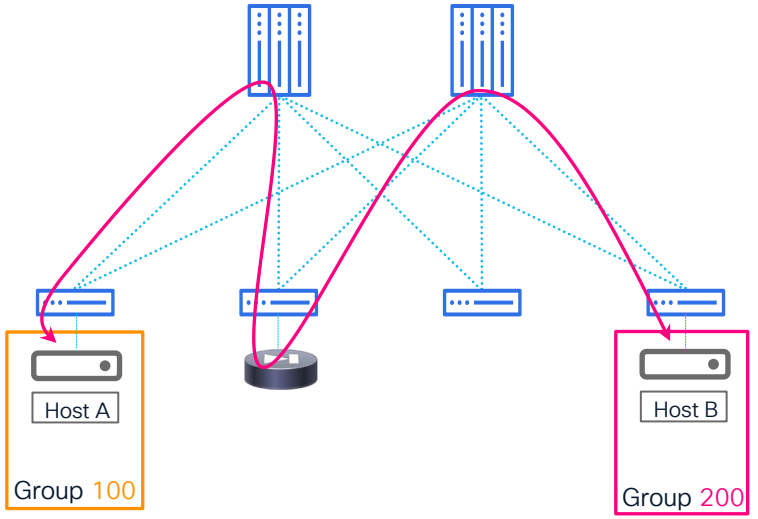
Segmentation

- Policies for macro and micro segmentation
- Control N/S and E/W traffic
- Granular filtering and better resource utilization



Service Redirection

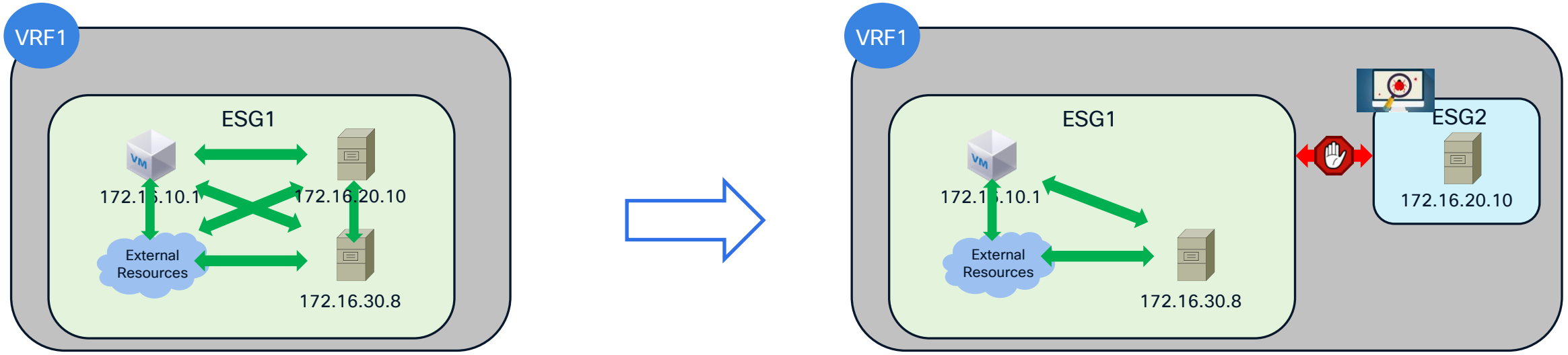
- Easily insert service devices in the traffic path
- Traffic can be steered w/o touching routing tables or creating complex network designs



© 2025 Cisco and/or its affiliates. All rights reserved.

VXLAN GPO with NX-OS

Use Case - VRF as a Security Zone



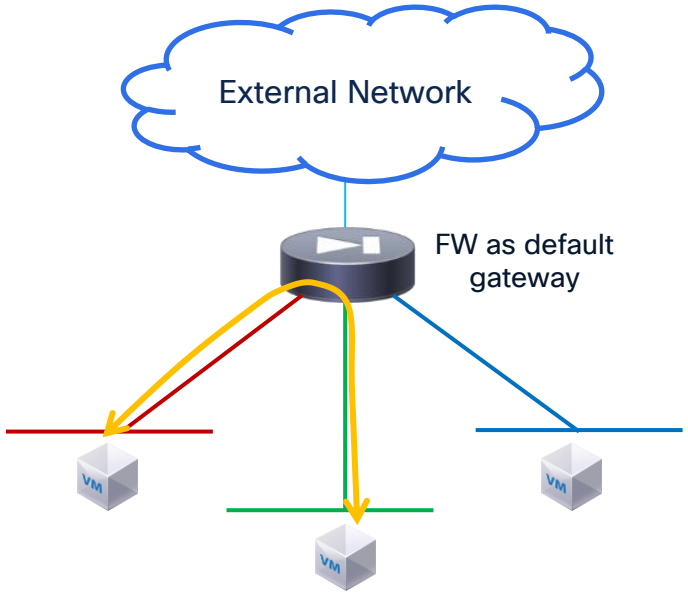
- Creation of a single security group to classify endpoints connected to all the networks (internal and external) part of the same VRF
- Provides intra-VRF open connectivity

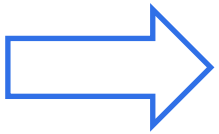
- Easy way to segment out specific endpoints that needs to get isolated (for example because they got compromised)

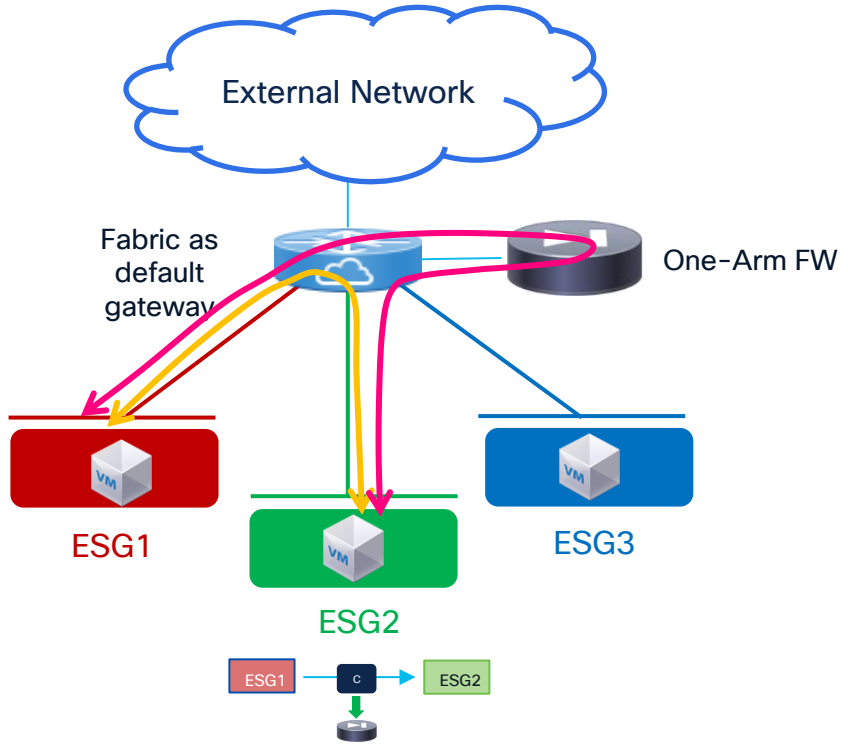
© 2025 Cisco and/or its affiliates. All rights reserved.

VXLAN GPO with NX-OS

Use Case - Subnet as a Security Zone







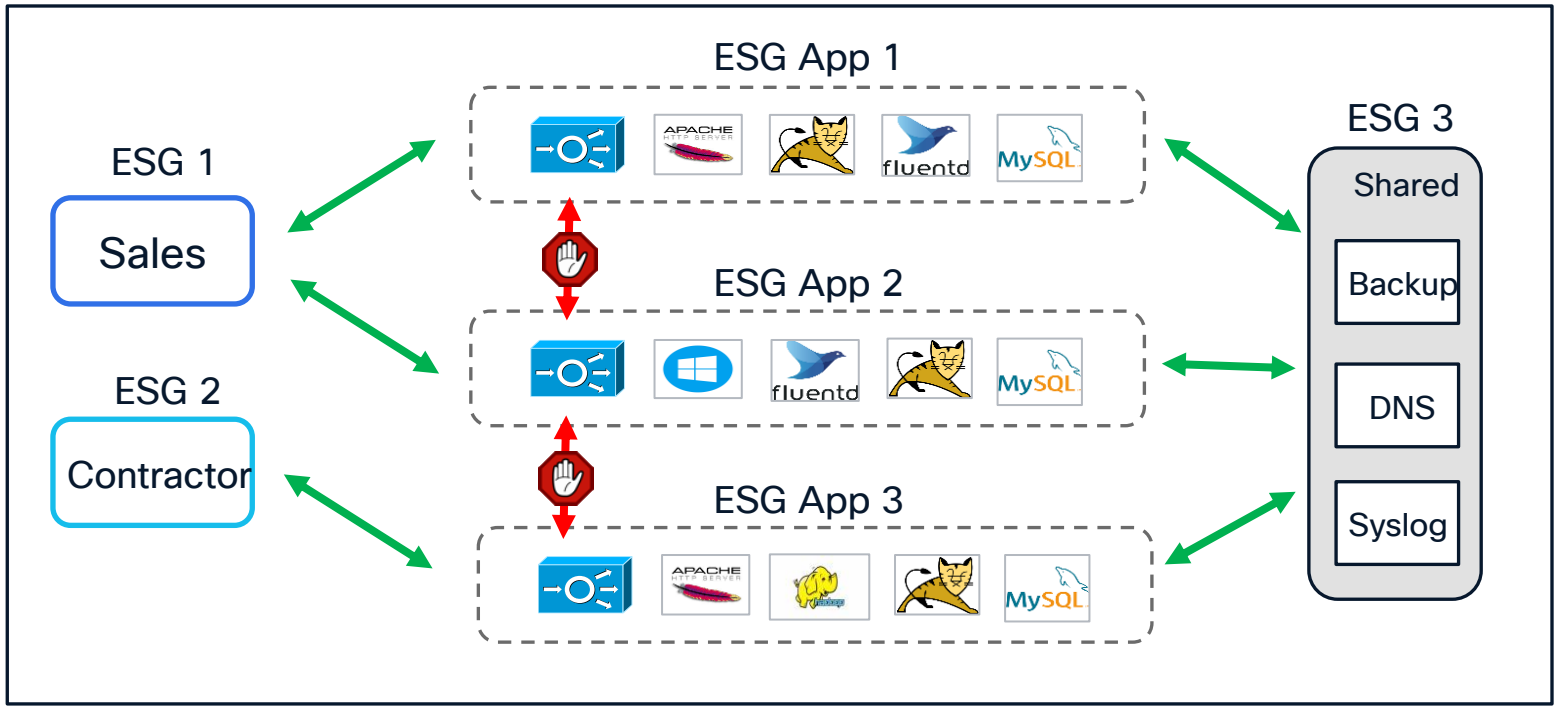
- Traditional design requires the deployment of a firewall as default gateway
- All inter-subnet flows are forced through the firewall, which may become a bottleneck

- Moving the default gateway function on the fabric
- Defining a separate ESG per subnet
- Redirect selective inter-subnet traffic flows only through the firewall, enforce policy or simply route at the fabric level for the rest of the flows

© 2025 Cisco and/or its affiliates. All rights reserved.

VXLAN GPO with NX-OS

Use Case – Application as a Security Zone



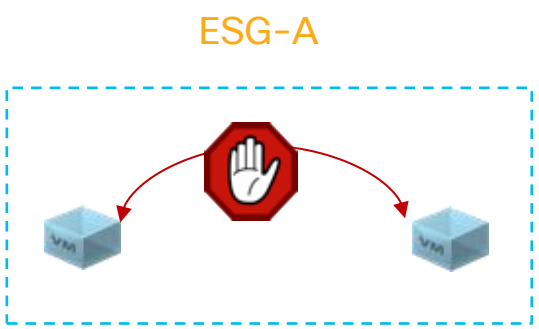
- Application as a security zone
- Does not require to know how the various components of the same application interact with each other
- Control communication between users and app, app to app and app to shared services

© 2025 Cisco and/or its affiliates. All rights reserved.

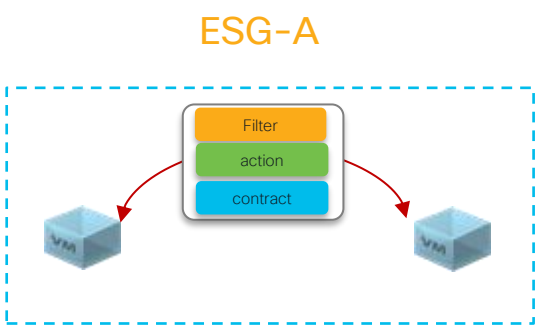
VXLAN GPO with NX-OS

Upcoming Use Cases*

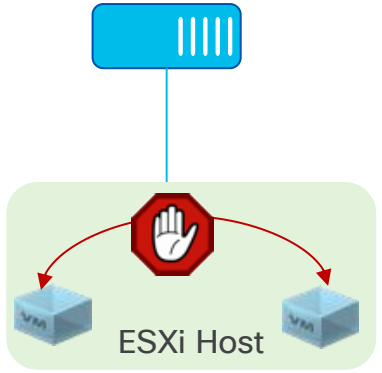
Intra-group Isolation



Intra-group Contract



Policy enforcement between endpoints connected to a common southbound Layer 2 switch (physical or virtual)



*Planned to be addressed in the 10.6(x) train

© 2025 Cisco and/or its affiliates. All rights reserved.

Group Policy Option

Compatibility and Licensing

Licensing: Essentials

GPO introduced in NX-OS 10.4(3)F

- FX3, GX and GX2 platforms*
- Single and Multi Site** Fabrics

NX-OS 10.5(1)F introduced

- 9408 platform*
- Single Service Function Redirection in Single Fabrics

NX-OS 10.5(2)F introduced

- FX, FX2 and HX platforms*
- Multi Service Function Redirection in Single and Multi-Site** Fabrics
- IPv6 in Underlay

NX-OS 10.5(3)F introduced

- New Classifiers and ISSU support

*Min 24G RAM

**Multi-Site requires Advantage on BGWs

© 2025 Cisco and/or its affiliates. All rights reserved.

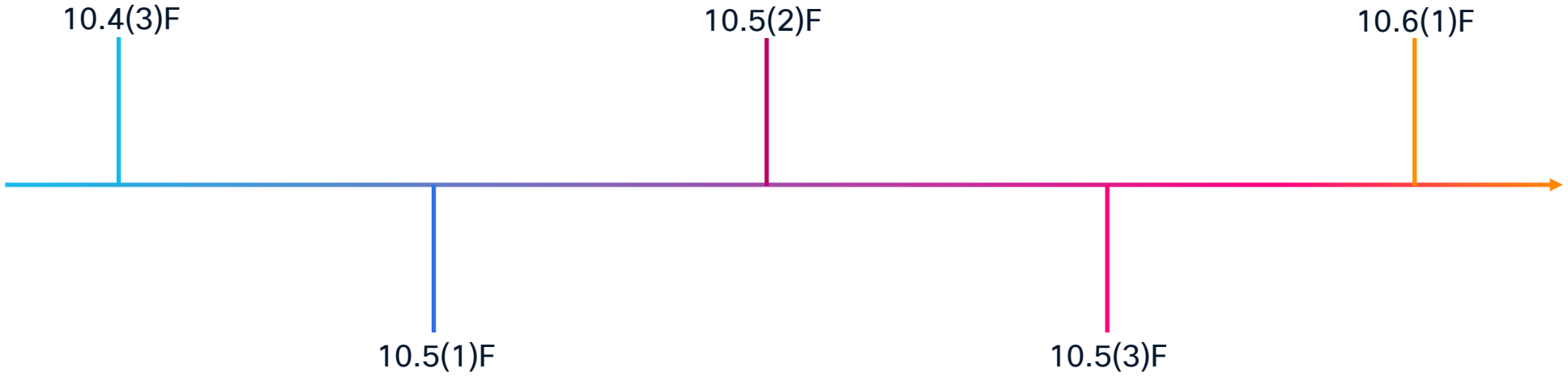
Group Policy Option

Feature Evolution

- Single and Multi-Site
- Supported Platforms: FX3, GX, GX2
- Classifiers: IP, VLAN
- Actions: Permit/Deny
- Single Site and Multi-Site

- Supported Platforms: FX. FX2, HX
- Actions: Redirection to Multi-Site
- IPv6 Underlay

- Classifiers: (Port,VLAN)
- MAC based micro-segmentation



- Supported Platforms: 9408
- Actions: Redirection to Single-Site

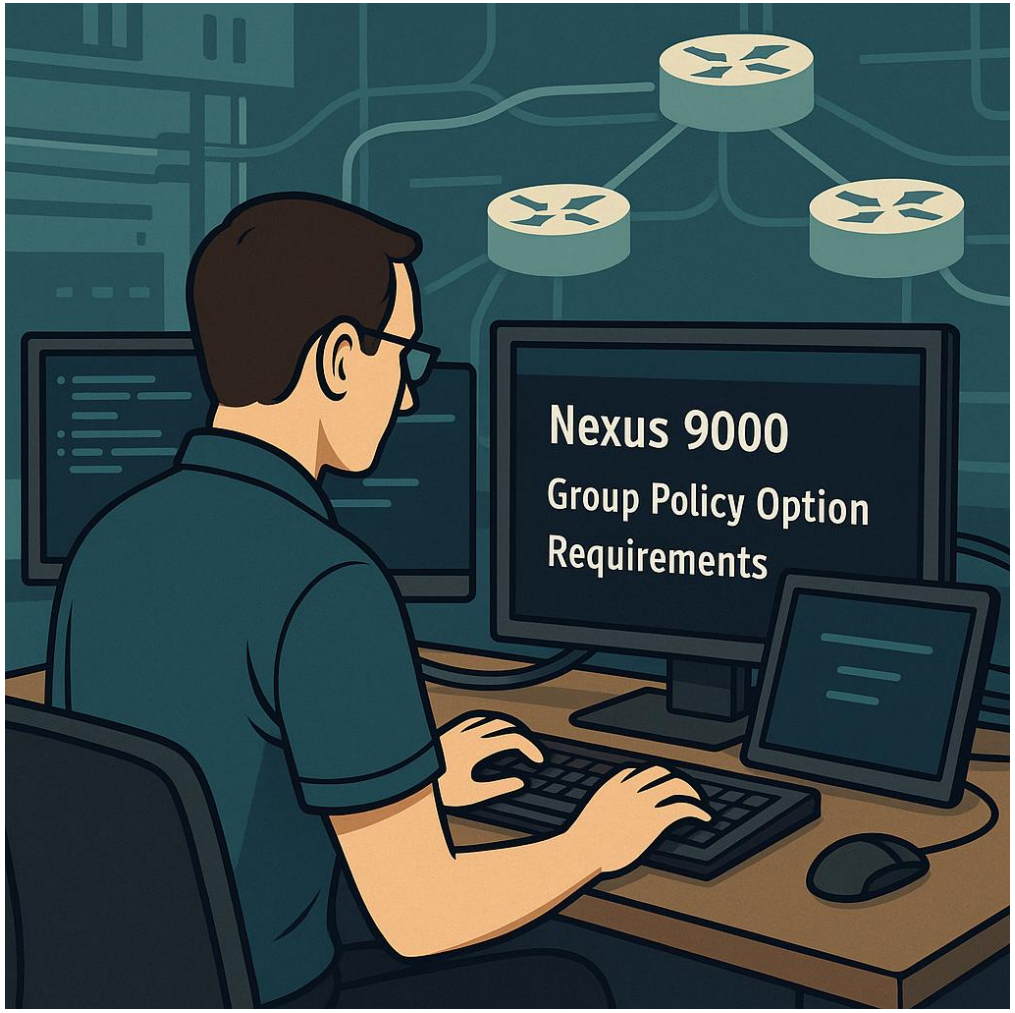
- Classifiers: MAC address
- ISSU Support
- N/S traffic via SR-MPLS

© 2025 Cisco and/or its affiliates. All rights reserved.

Group Policy Option

Device Requirements

- Devices require minimum 24G of RAM
- Essentials License provides access to every GPO related functionality:
  - Basic enforcement
  - Redirection
- NX-OS requires some ad-hoc configs that will require a (single) reload:
  - Routing Template: system routing template-security-groups
  - SSD repartitioning: system flash sda resize extended
  - GPO feature: feature security-group

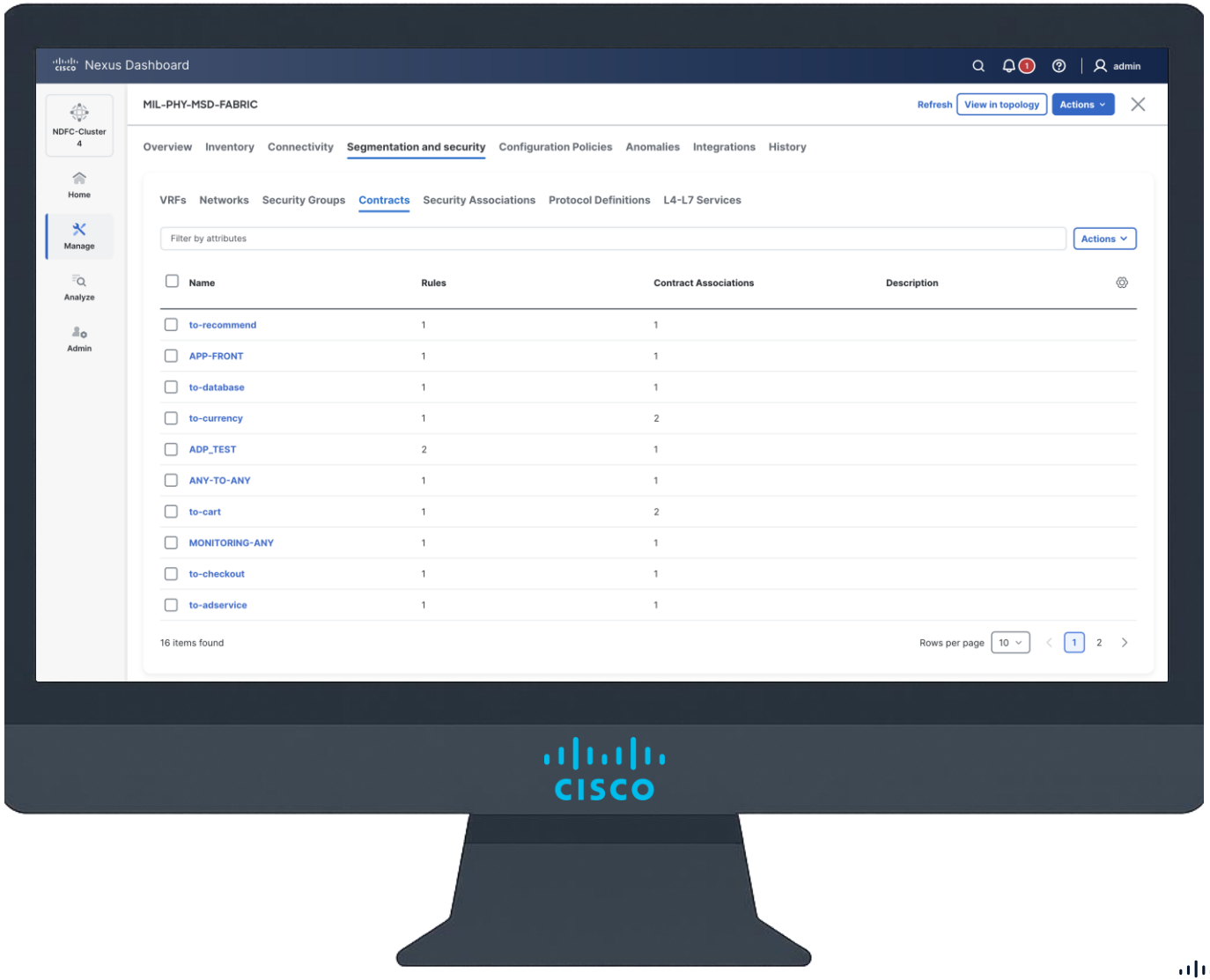


© 2025 Cisco and/or its affiliates. All rights reserved.

Group Policy Option

Controller Requirements

- Nexus Dashboard is highly recommended but optional
- Support for GPO added in ND 3.2
- Supports Single-Site and Multi-Site environments
- Seamless workflows to help administrators define the Data Center security posture
- Many enhancements will be added in upcoming versions



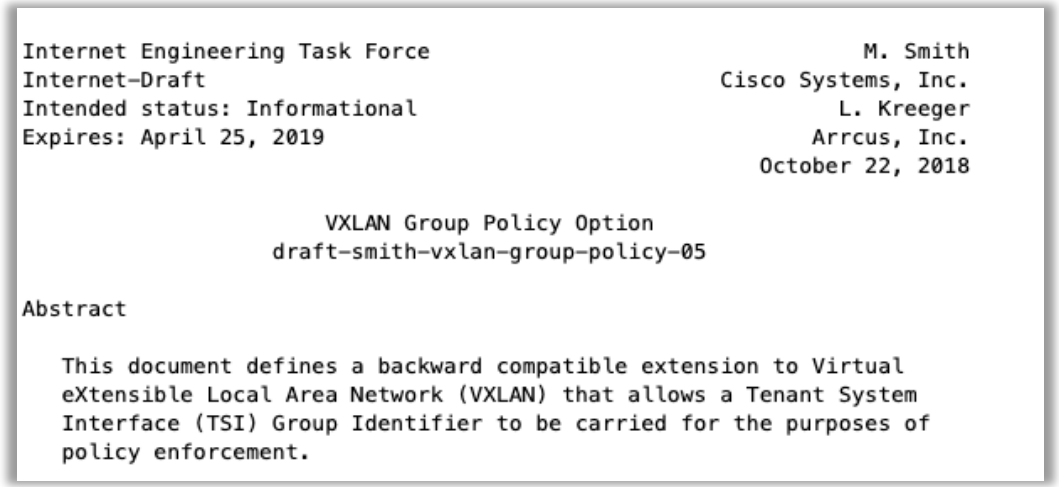
© 2025 Cisco and/or its affiliates. All rights reserved.

GPO Origin

Group Policy Option

Origin – IETF Drafts – Data Plane

- Originally defined in 2014, introduces backward compatible options to carry additional values in the VXLAN header
- Values include a Security Group Tag (SGT) and a few additional flags
- These values can be written and read by ingress and egress VTEPs to enforce security rules on overlay traffic
- Not widely adopted due to the lack of a related Control Plane
- No Control Plane = Inefficient use of fabric bandwidth

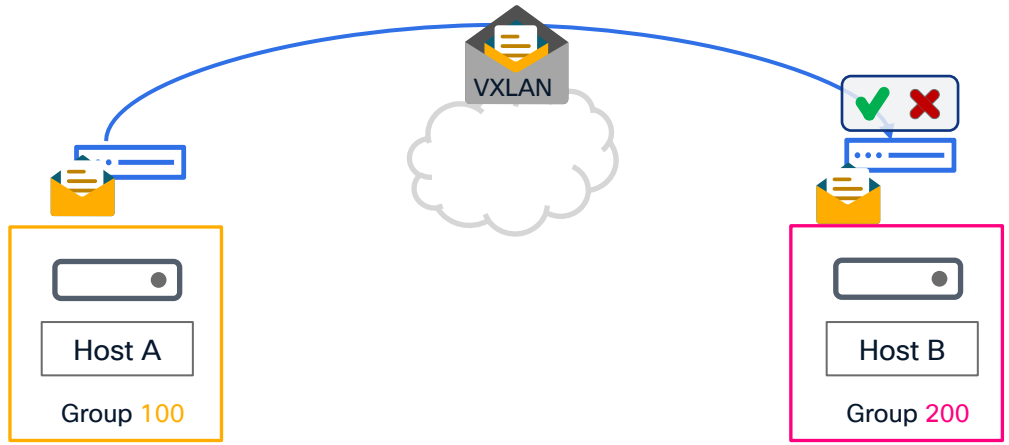


Internet Engineering Task Force — M. Smith
Internet-Draft — Cisco Systems, Inc.
Intended status: Informational — L. Kreeger
Expires: April 25, 2019 — Arrcus, Inc.
October 22, 2018

VXLAN Group Policy Option
draft-smith-vxlan-group-policy-05

Abstract

This document defines a backward compatible extension to Virtual eXtensible Local Area Network (VXLAN) that allows a Tenant System Interface (TSI) Group Identifier to be carried for the purposes of policy enforcement.

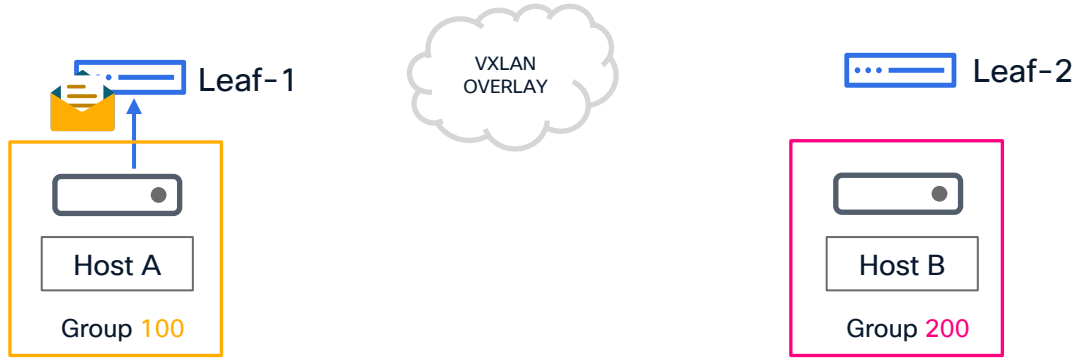


© 2025 Cisco and/or its affiliates. All rights reserved.

Group Policy Option

Origin – IETF Drafts – Data Plane

- Ingress leaf receives a packet that needs to be forwarded in the overlay

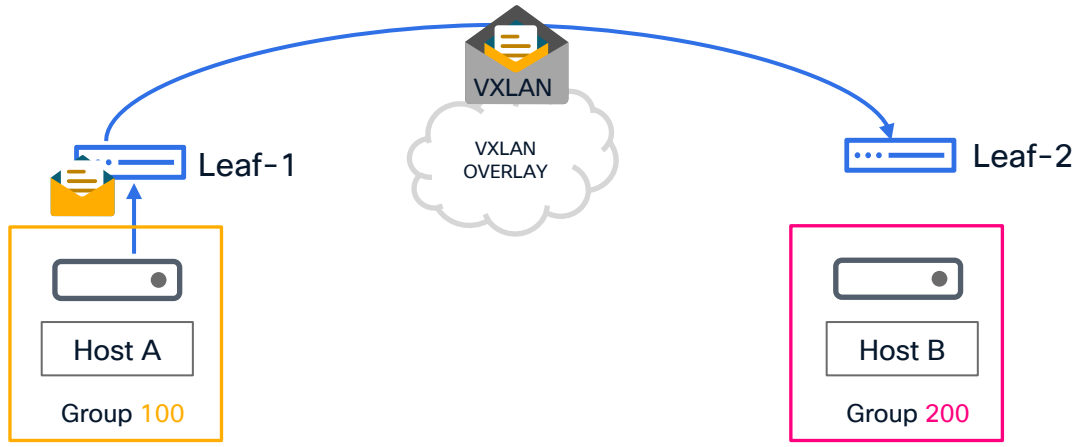


© 2025 Cisco and/or its affiliates. All rights reserved.

Group Policy Option

Origin – IETF Drafts – Data Plane

- Ingress leaf receives a packet that needs to be forwarded in the overlay
- Ingress leaf encapsulates the original packet into a VXLAN-GPO one and sends it to the egress VTEP



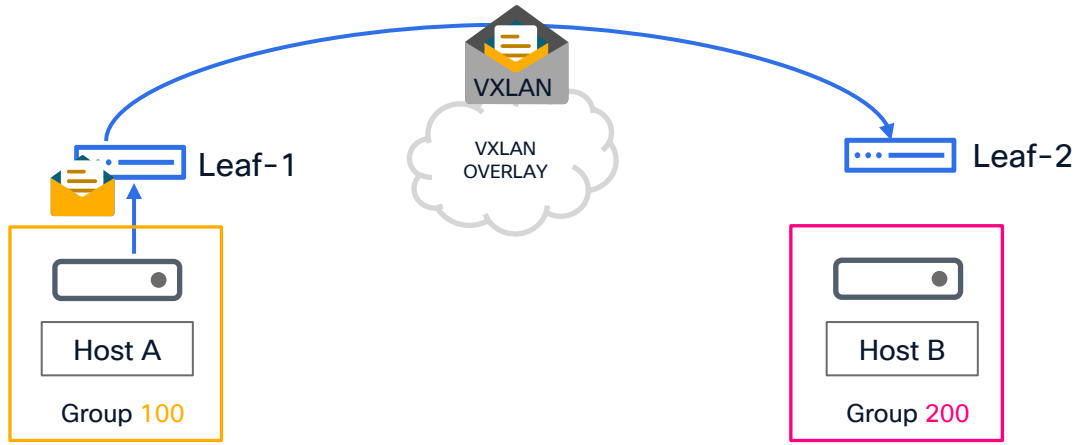
© 2025 Cisco and/or its affiliates. All rights reserved.

Group Policy Option

Origin – IETF Drafts – Data Plane

- Ingress leaf receives a packet that needs to be forwarded in the overlay
- Ingress leaf encapsulates the original packet into a VXLAN-GPO one and sends it to the egress VTEP
- Ingress Leaf is GPO aware, and has an SGT mapping for the source end-host
  - 1st bit (GBP Extension) = 1
  - SGT = 100
  - 12th bit (Policy Applied) = 0

```
Virtual eXtensible Local Area Network
 Flags: 0xc810, GBP Extension, VXLAN Network ID (VNI)
   1... .... .... .... = GBP Extension: Defined
   .... 1... .... .... = VXLAN Network ID (VNI): True
   .... .... .0.. .... = Don't Learn: False
   .... .... .... 0... = Policy Applied: False
   .100 .000 0.01 .000 = Reserved(R): 0x4010
 Group Policy ID: 100
 VXLAN Network Identifier (VNI): 2097152
 Reserved: 0
```



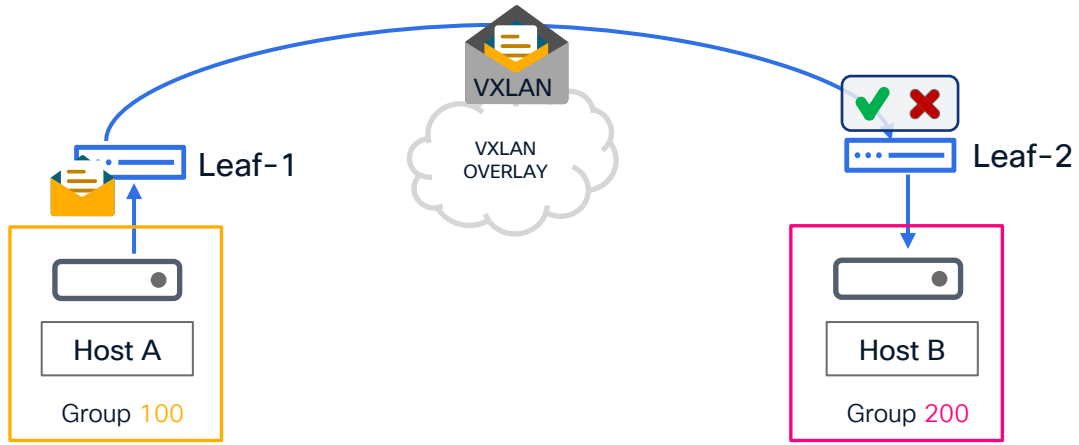
© 2025 Cisco and/or its affiliates. All rights reserved.

Group Policy Option

Origin – IETF Drafts – Data Plane

- Ingress leaf receives a packet that needs to be forwarded in the overlay
- Ingress leaf encapsulates the original packet into a VXLAN-GPO one and sends it to the egress VTEP
- Ingress Leaf is GPO aware, and has an SGT mapping for the source end-host
  - 1st bit (GBP Extension) = 1
  - SGT = 100
  - 12th bit (Policy Applied) = 0
- VXLAN packet is received from egress VTEP who knows the destination end-host SGT
  - Policy can be applied there

```
Virtual eXtensible Local Area Network
 Flags: 0xc810, GBP Extension, VXLAN Network ID (VNI)
   1... .... .... .... = GBP Extension: Defined
   .... 1... .... .... = VXLAN Network ID (VNI): True
   .... .... .0.. .... = Don't Learn: False
   .... .... .... 0... = Policy Applied: False
   .100 .000 0.01 .000 = Reserved(R): 0x4010
 Group Policy ID: 100
 VXLAN Network Identifier (VNI): 2097152
 Reserved: 0
```



© 2025 Cisco and/or its affiliates. All rights reserved.

Group Policy Option

Origin – IETF Drafts – Control Plane

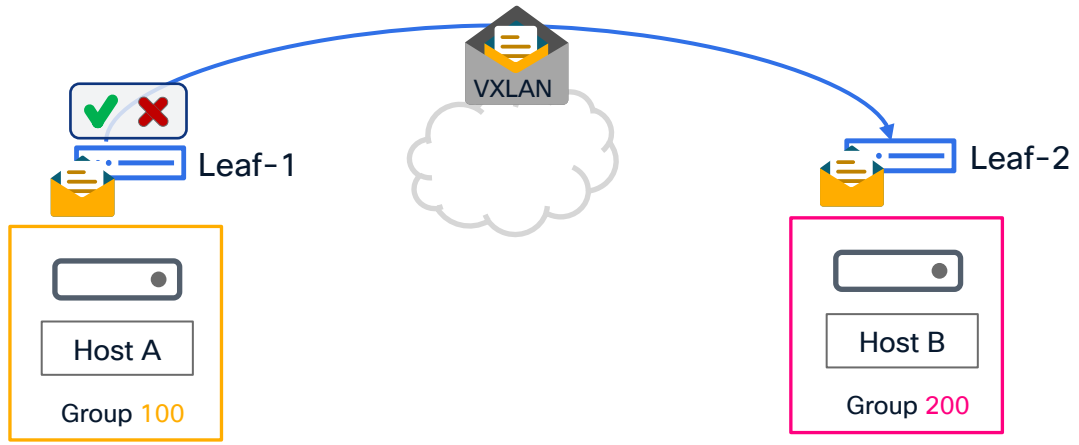
- Originally defined in 2022
- Defines an additional BGP extended community that can be appended to EVPN advertisements
- The extended community, which is set by the advertising VTEP to route types-[2-3-5], contains the SGT value
- Ingress leaf get to know the destination EP SGT and can enforce the traffic locally (data plane)
- The action is also signalled to the egress node so it can skip the policy enforcement (data plane)

bess W. Lin
Internet-Draft Juniper Networks
Intended status: Standards Track J. Drake
Expires: 22 April 2024 Individual
D. Rao
Cisco Systems
20 October 2023

Group Policy ID BGP Extended Community
draft-wlin-bess-group-policy-id-extended-community-03

Abstract

Group Based Policy can be used to achieve micro or macro segmentation of user traffic. For Group Based Policy, a Group Policy ID, also known as Group Policy Tag, is used to represent a logical group that shares the same policy and access privilege. This specification defines a new BGP extended community that can be used to propagate Group Policy ID through a BGP route advertisement in the control plane. This is to facilitate policy enforcement at the ingress node when the optimization of network bandwidth is desired.



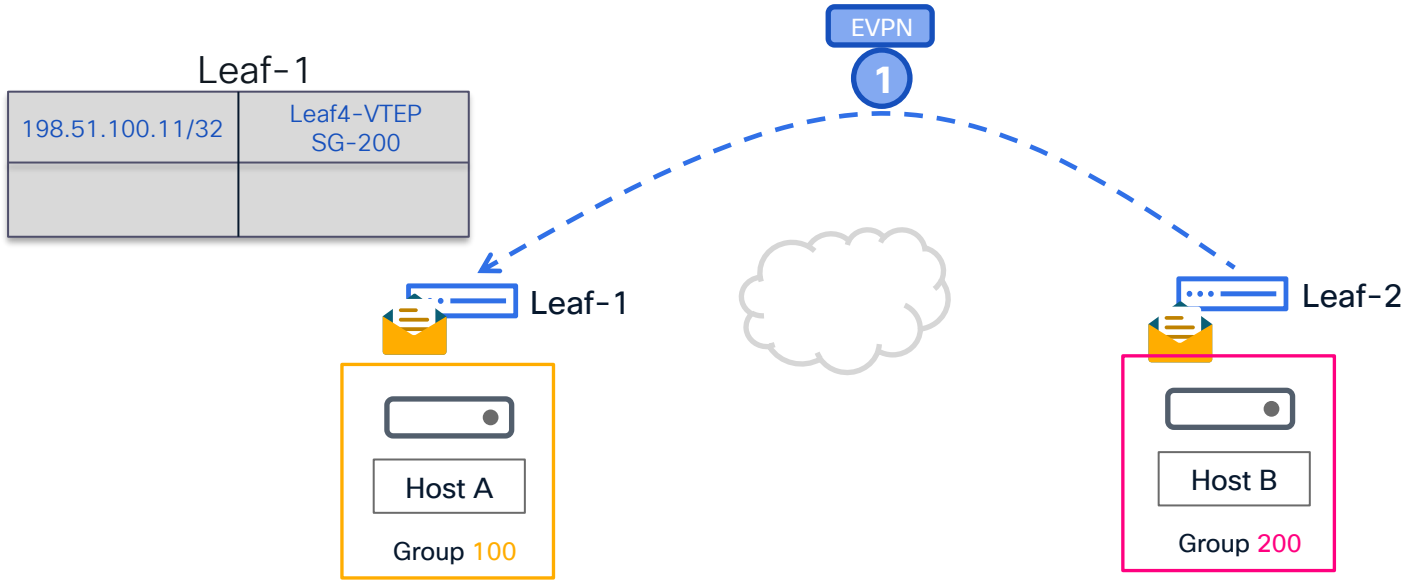
© 2025 Cisco and/or its affiliates. All rights reserved.

Group Policy Option

Origin – IETF Drafts – Control Plane - Flow

- When an endpoint or an external route is discovered, it gets redistributed in EVPN together with its SGT
- The propagation of such EVPN NLRI allows the remote VTEPs to learn about remote endpoints and routes together with their SGT

```
Path type: internal, path is valid, is best path
 Imported to 3 destination(s)
 Imported paths list: legacy_vrf L3-15002 L2-12112
 AS-Path: NONE, path sourced internal to AS
  172.20.21.3 (metric 3) from 172.20.20.2 (172.20.20.2)
    Origin IGP, MED not set, localpref 100, weight 0
    Received label 12112 15002
    Extcommunity: RT:65102:12112 RT:65102:15002 PCTAG:0:0:200
    ENCAP:8 MAC Mobility Seq:00:2 Router MAC:748f.c291.ac07
    Originator: 172.20.20.4 Cluster list: 172.20.20.2
```



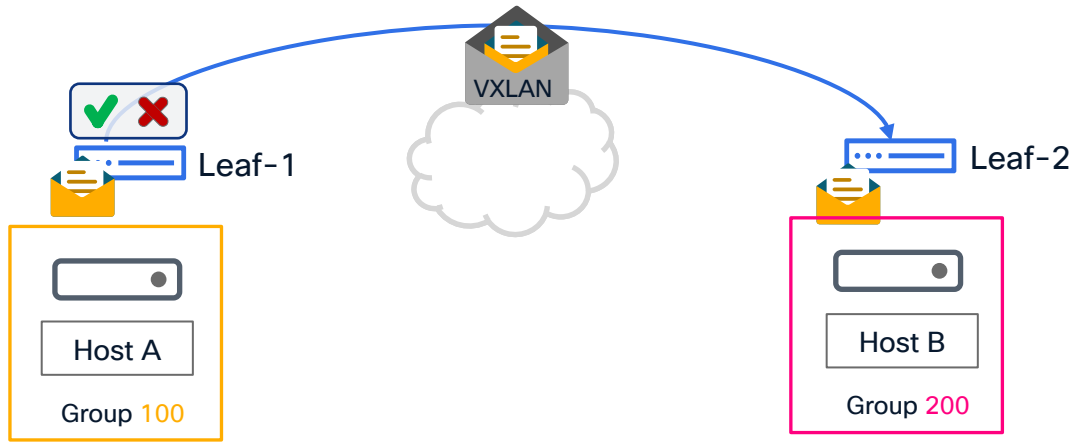
© 2025 Cisco and/or its affiliates. All rights reserved.

Group Policy Option

Origin – IETF Drafts – Control Plane - Flow

- When an endpoint or an external route is discovered, it gets redistributed in EVPN together with its SGT
- The propagation of such EVPN NLRI allows the remote VTEPs to learn about remote endpoints and routes together with their SGT
- (Data Plane) - Now the ingress leaf can immediately apply the policy
- If traffic is allowed, original packet will be encapsulated in a VXLAN-GPO packet
  - 1st bit (GBP Extension) = 1
  - SGT = 100
  - 12th bit (Policy Applied) = 1

```
Virtual eXtensible Local Area Network
  Flags: 0xc818, GBP Extension, VXLAN Network ID (VNI), Policy Applied
    1... .... .... .... = GBP Extension: Defined
    .... 1... .... .... = VXLAN Network ID (VNI): True
    .... .... .0.. .... = Don't Learn: False
    .... .... .... 1... = Policy Applied: True
    .100 .000 0.01 .000 = Reserved(R): 0x4010
  Group Policy ID: 100
  VXLAN Network Identifier (VNI): 2097152
  Reserved: 0
```



© 2025 Cisco and/or its affiliates. All rights reserved.

Group Policy Option

Origin – IETF Drafts – Combined Data and Control Plane

Data Plane
(draft-smith-vxlan-group-policy)

Internet Engineering Task Force
Internet-Draft
Intended status: Informational
Expires: April 25, 2019

M. Smith
Cisco Systems, Inc.
L. Kreeger
Arrcus, Inc.
October 22, 2018

VXLAN Group Policy Option
draft-smith-vxlan-group-policy-05

Abstract

This document defines a backward compatible extension to Virtual eXtensible Local Area Network (VXLAN) that allows a Tenant System Interface (TSI) Group Identifier to be carried for the purposes of policy enforcement.

+

Control Plane
(draft-wlin-bess-group-policy-id-extended-community)

bess
Internet-Draft
Intended status: Standards Track
Expires: 22 April 2024

W. Lin
Juniper Networks
J. Drake
Individual
D. Rao
Cisco Systems
20 October 2023

Group Policy ID BGP Extended Community
draft-wlin-bess-group-policy-id-extended-community-03

Abstract

Group Based Policy can be used to achieve micro or macro segmentation of user traffic. For Group Based Policy, a Group Policy ID, also known as Group Policy Tag, is used to represent a logical group that shares the same policy and access privilege. This specification defines a new BGP extended community that can be used to propagate Group Policy ID through a BGP route advertisement in the control plane. This is to facilitate policy enforcement at the ingress node when the optimization of network bandwidth is desired.

Data Plane and Control Plane
(draft-lrss-bess-evpn-group-policy)

BESS WorkGroup
Internet-Draft
Intended status: Standards Track
Expires: 24 April 2025

W. Lin
Juniper
D. Rao
A. Sajassi
M. Smith
Cisco
L. Kreeger
Arrcus
J. Rabadan
Nokia
21 October 2024

EVPN Group Policy
draft-lrss-bess-evpn-group-policy-01

Abstract

Group Based Policy can be used to achieve micro or macro segmentation of user traffic. For Group Based Policy, a Group Policy ID, also known as Group Policy Tag, is used to represent a logical group that shares the same policy and access privilege. This document defines a backward compatible extension to Virtual eXtensible Local Area Network (VXLAN) that allows a Group Policy ID to be carried for the purposes of policy enforcement at the egress Network Virtualization Edge (NVE). It also defines a new BGP Extended Community that can be used to propagate Group Policy ID through a BGP route advertisement in the control plane. This is to facilitate policy enforcement at the ingress NVE when feasible.

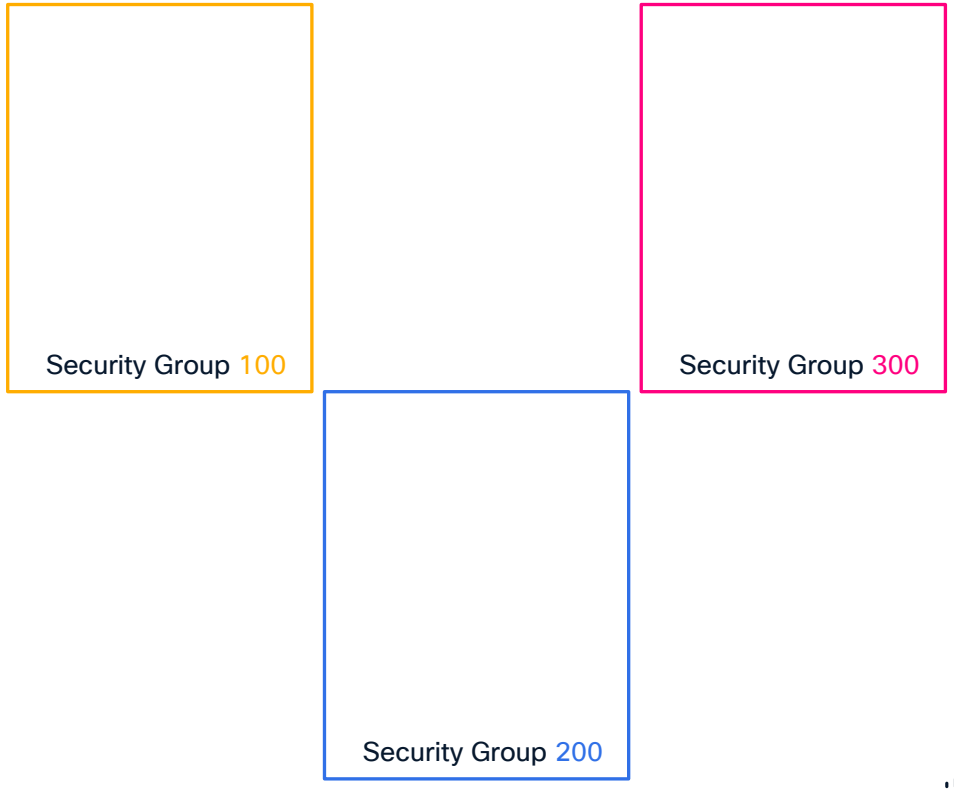
© 2025 Cisco and/or its affiliates. All rights reserved.

GPO Fundamentals

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 can be enforced
- Common reserved SGs:
  - 0 – for any non classified address, also refer to as “any”
  - 1 – for default type-5 routes of directly connected networks
  - 15 – prefixes learned from GPO unaware sites

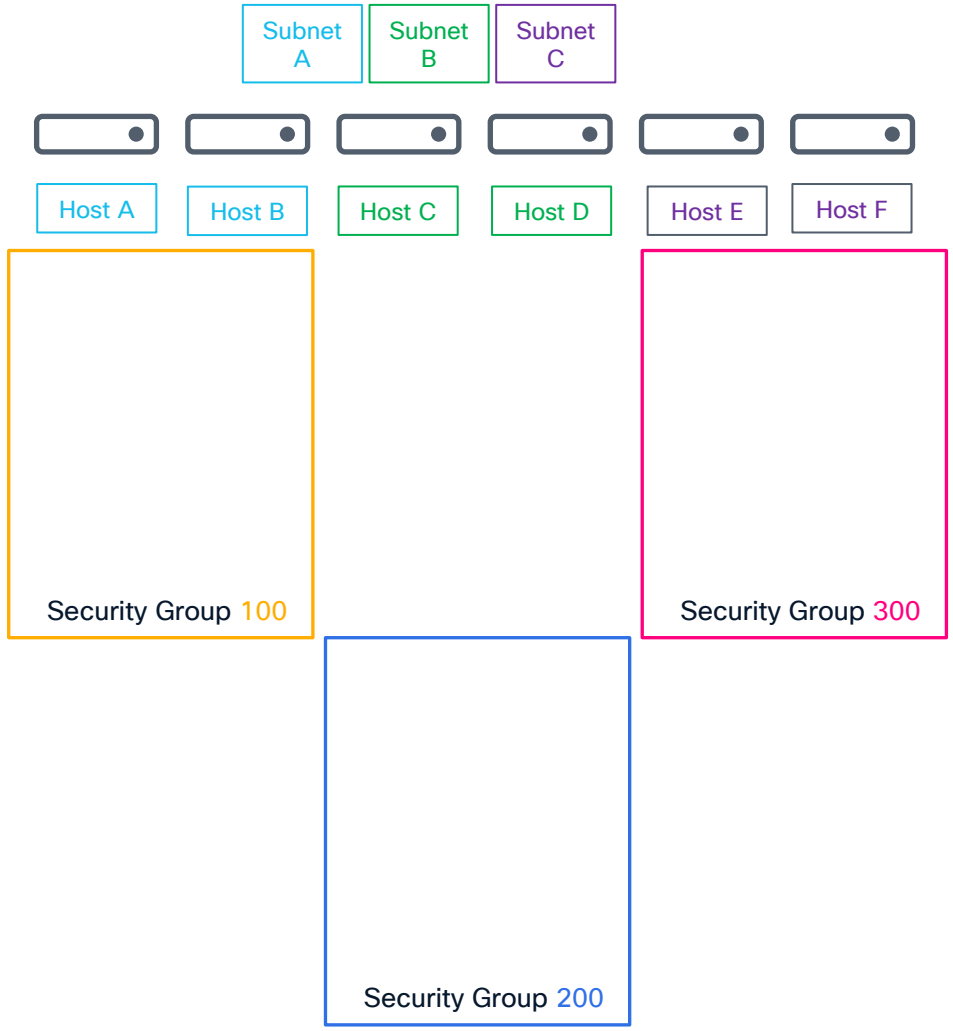


© 2025 Cisco and/or its affiliates. All rights reserved.

Group Policy Option Fundamentals

Endpoint Classification

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



© 2025 Cisco and/or its affiliates. All rights reserved.

Group Policy Option Fundamentals

Endpoint Classification

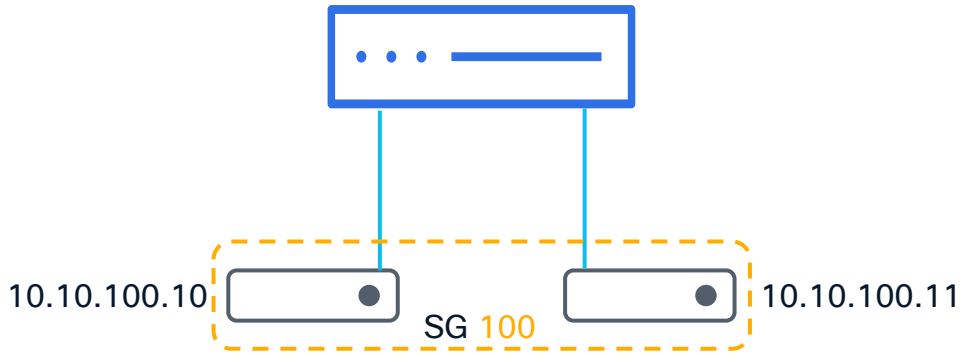
- Classification, is done in CLI and depends on resource type
  - Connected Endpoints:
    - IP based classification
      - LPMs (including host-routes)
    - VLAN based classification
    - MAC based classification
  - External Networks
    - IP Based Classification
      - LPMs
- Endpoints in the same subnet can be mapped to different or same SGs
- Endpoint in different subnets can be mapped to the same SG

© 2025 Cisco and/or its affiliates. All rights reserved.

Group Policy Option Fundamentals

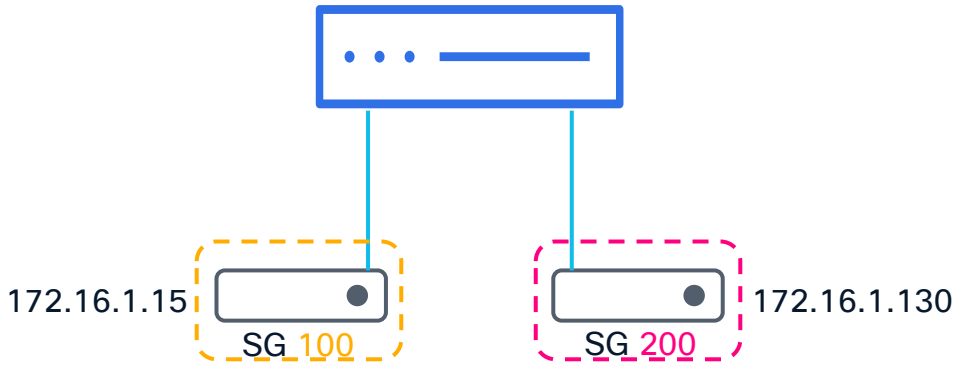
Connected Endpoint Classification – IP Based

Host Route Classifier




```
security-group 100 name MY_SG_1
  match connected-endpoints vrf my_vrf ipv4 10.10.100.10/32
  match connected-endpoints vrf my_vrf ipv4 10.10.100.11/32
```

LPM Classifier



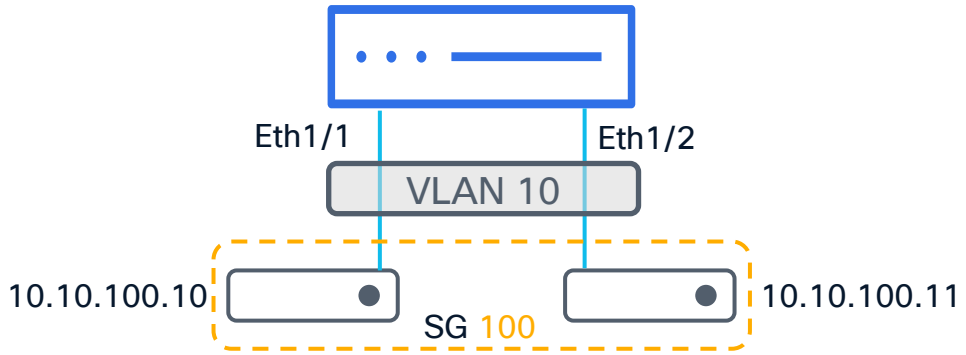

```
security-group 100 name MY_SG_1
  match connected-endpoints vrf my_vrf ipv4 172.16.1.0/24
security-group 200 name MY_SG_2
  match connected-endpoints vrf my_vrf ipv4 172.16.1.128/26
```

© 2025 Cisco and/or its affiliates. All rights reserved.

Group Policy Option Fundamentals

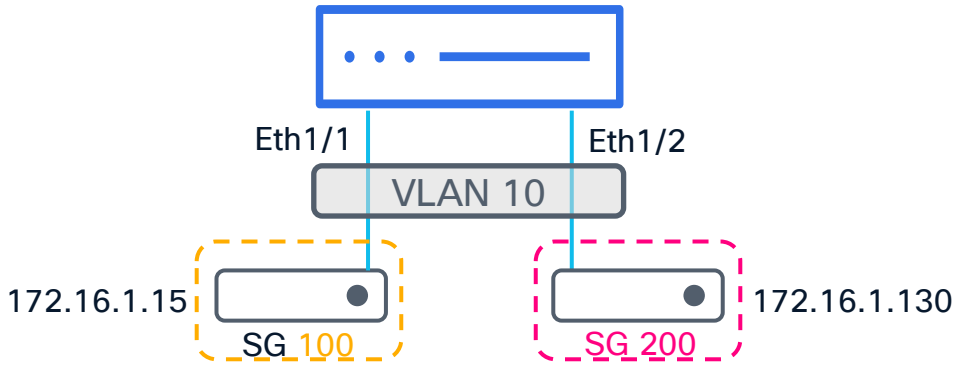
Connected Endpoint Classification – VLAN Based

VLAN Classifier




```
security-group 100 name MY_SG_1
  match vlan 10
```

(Port,VLAN) Classifier

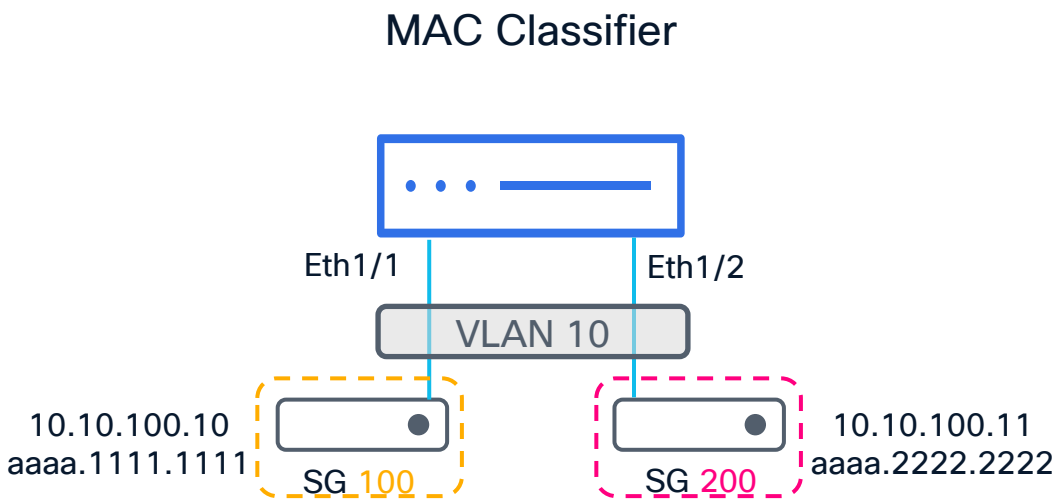



```
security-group 100 name MY_SG_1
  match vlan 10 interface eth1/1
security-group 200 name MY_SG_2
  match vlan 10 interface eth1/2
```

© 2025 Cisco and/or its affiliates. All rights reserved.

Group Policy Option Fundamentals

Connected Endpoint Classification – MAC Based

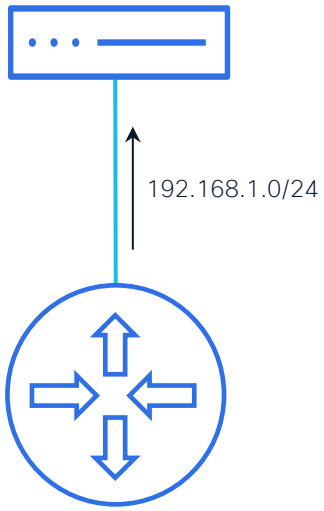



```
security-group 100 name MY_SG_1
  match vlan 10 mac aaaa.1111.1111
security-group 200 name MY_SG_2
  match vlan 10 mac aaaa.2222.2222
```

© 2025 Cisco and/or its affiliates. All rights reserved.

Group Policy Option Fundamentals

External Network Classifier



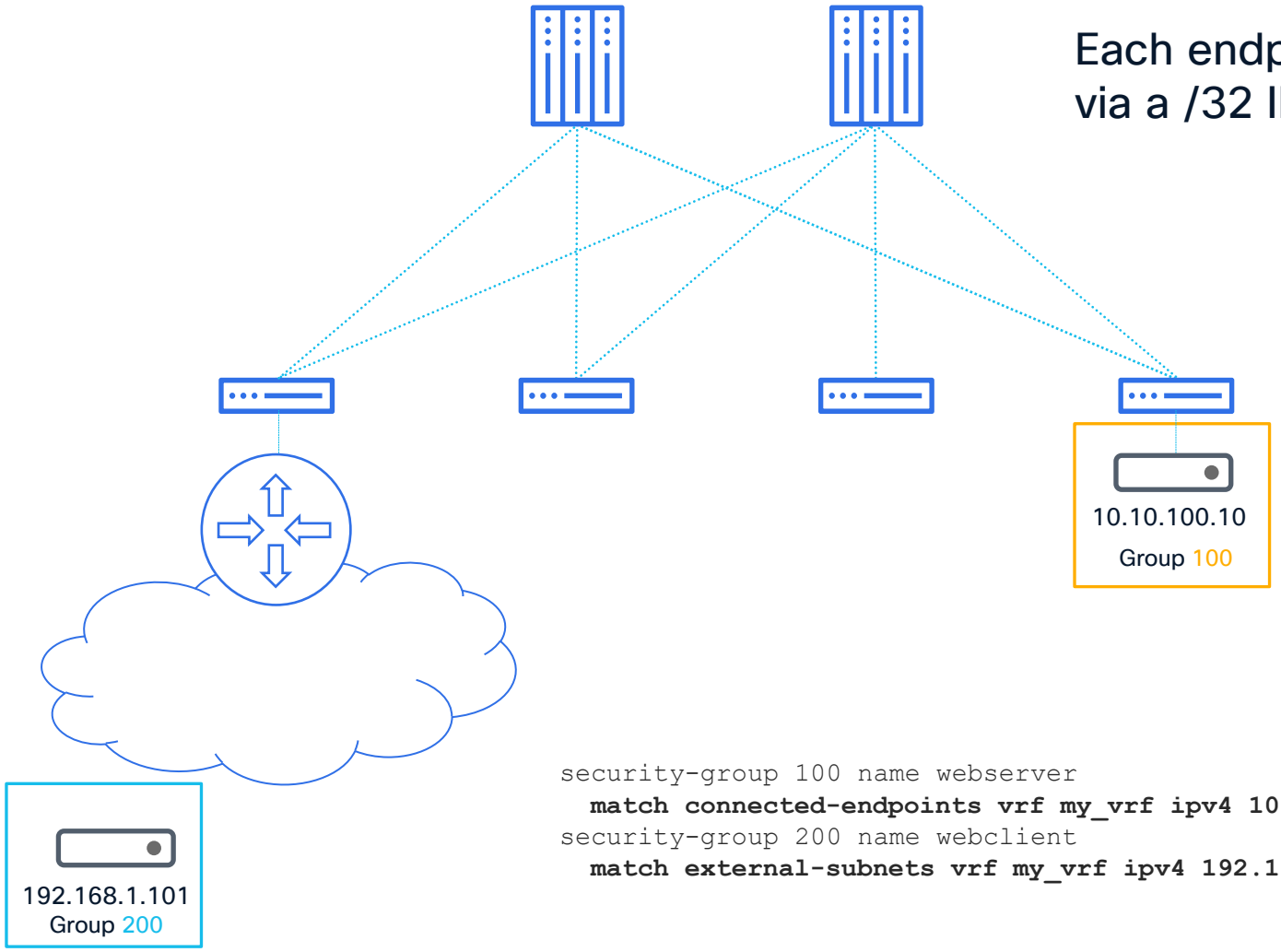
- External IPs or networks can be clasified into Security-Groups
- They can be learned via a dynamic protocol or programmed via static routes
- Classification is done at the border leaves and propagated to the fabric
- By default, security groups are attached to EVPN routes only when there's a classifier exactly matching the prefix or more specific than the prefix

```
security-group 200 name webclient
  match external-subnets vrf my_vrf ipv4 192.168.1.0/24
security-group 201 name appserver
  match external-subnets vrf my_vrf ipv4 192.168.1.101/32 route-inject
```

© 2025 Cisco and/or its affiliates. All rights reserved.

Group Policy Option Fundamentals

External Network Classifier – Broken Scenario



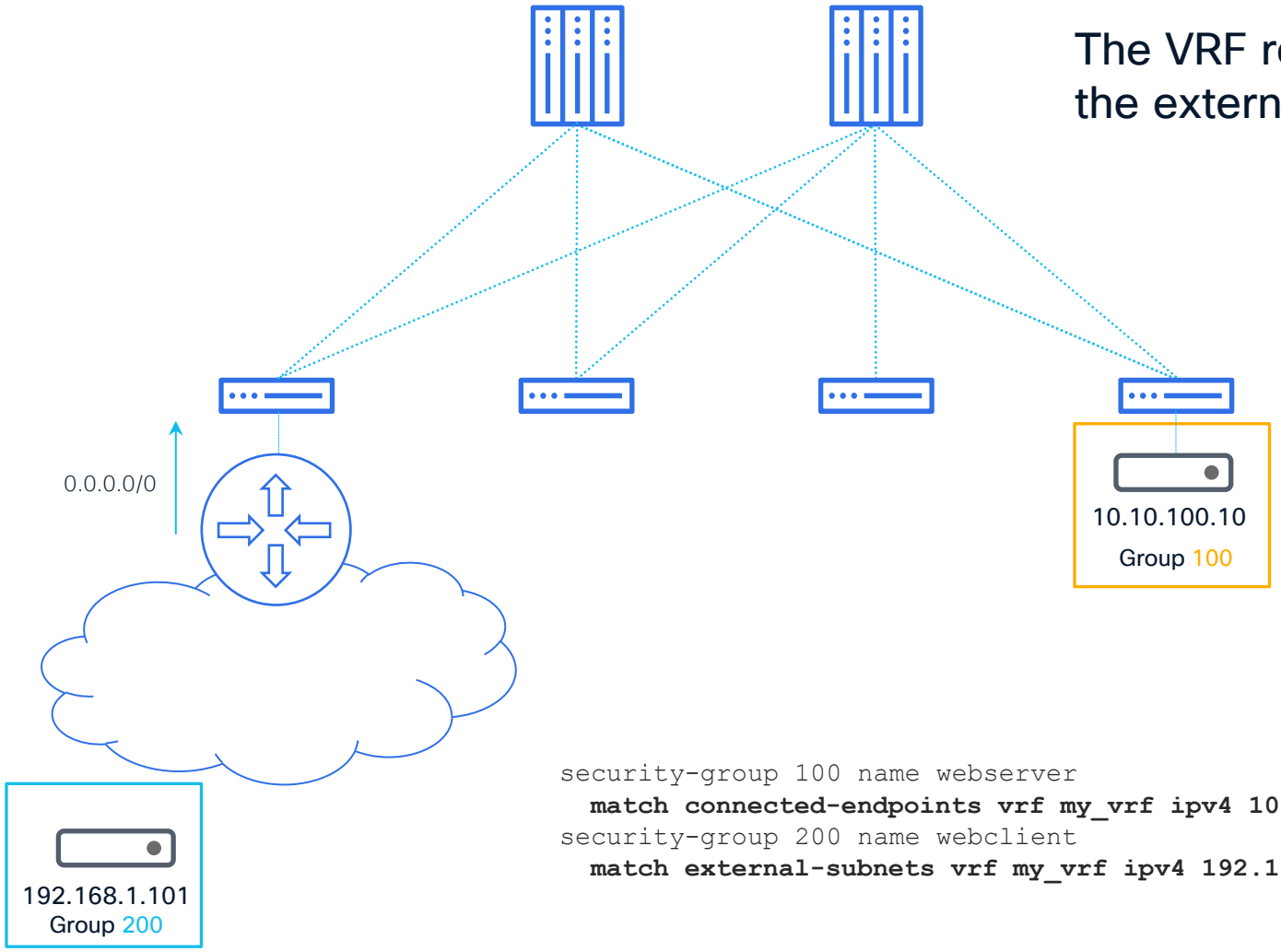
Each endpoint classification definition happens via a /32 IP address

```
security-group 100 name webserver
  match connected-endpoints vrf my_vrf ipv4 10.10.100.10/32
security-group 200 name webclient
  match external-subnets vrf my_vrf ipv4 192.168.1.101/32
```

© 2025 Cisco and/or its affiliates. All rights reserved.

Group Policy Option Fundamentals

External Network Classifier – Broken Scenario



The VRF receives only the default route from the external router

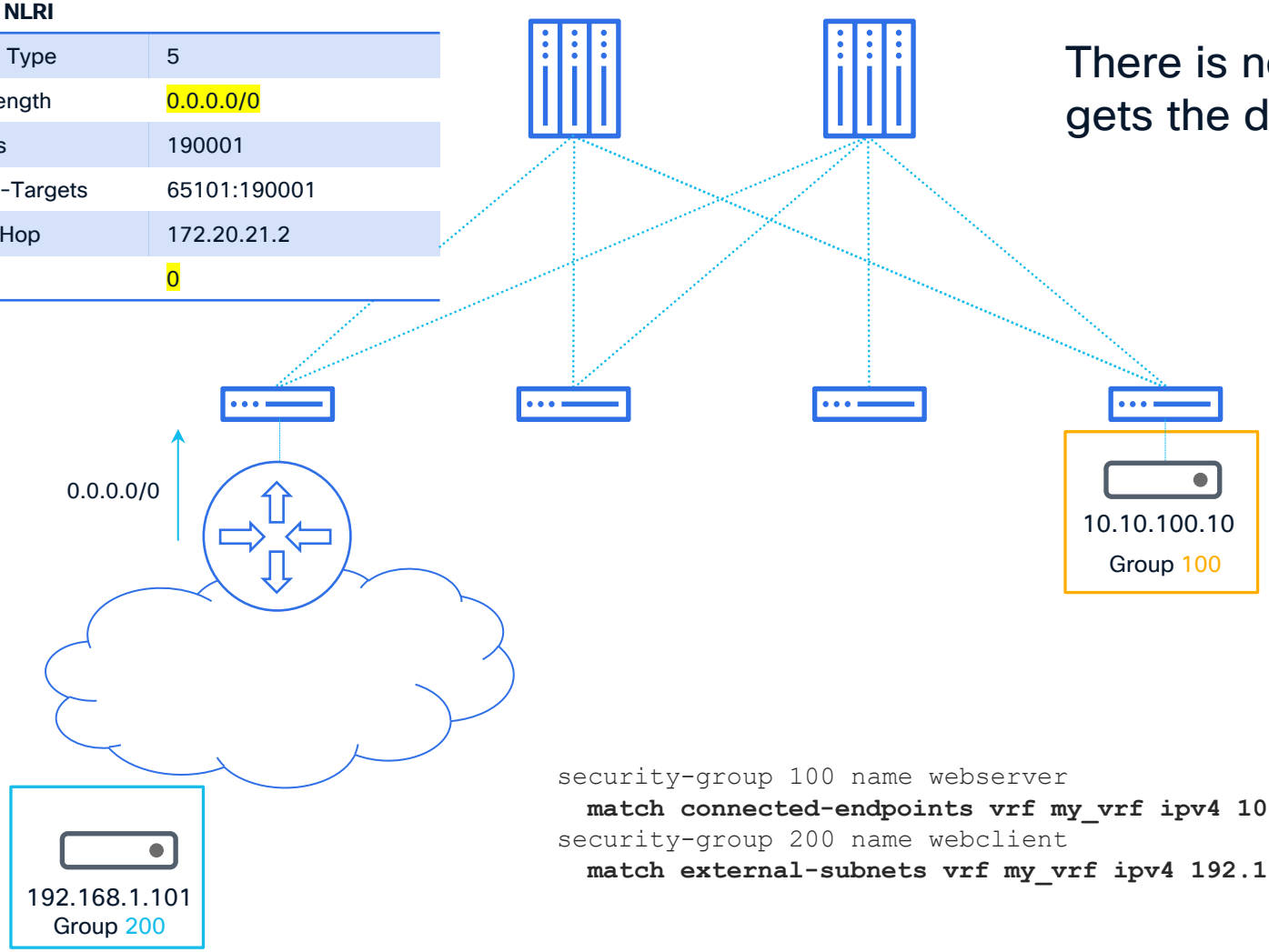
```
security-group 100 name webserver
  match connected-endpoints vrf my_vrf ipv4 10.10.100.10/32
security-group 200 name webclient
  match external-subnets vrf my_vrf ipv4 192.168.1.101/32
```

© 2025 Cisco and/or its affiliates. All rights reserved.

Group Policy Option Fundamentals

External Network Classifier – Broken Scenario

EVPN NLRI	
Route Type	5
IP / Length	0.0.0.0/0
Labels	190001
Route-Targets	65101:190001
Next-Hop	172.20.21.2
SGT	0



There is no classification for the 0.0.0.0/0, so it gets the default SGT 0

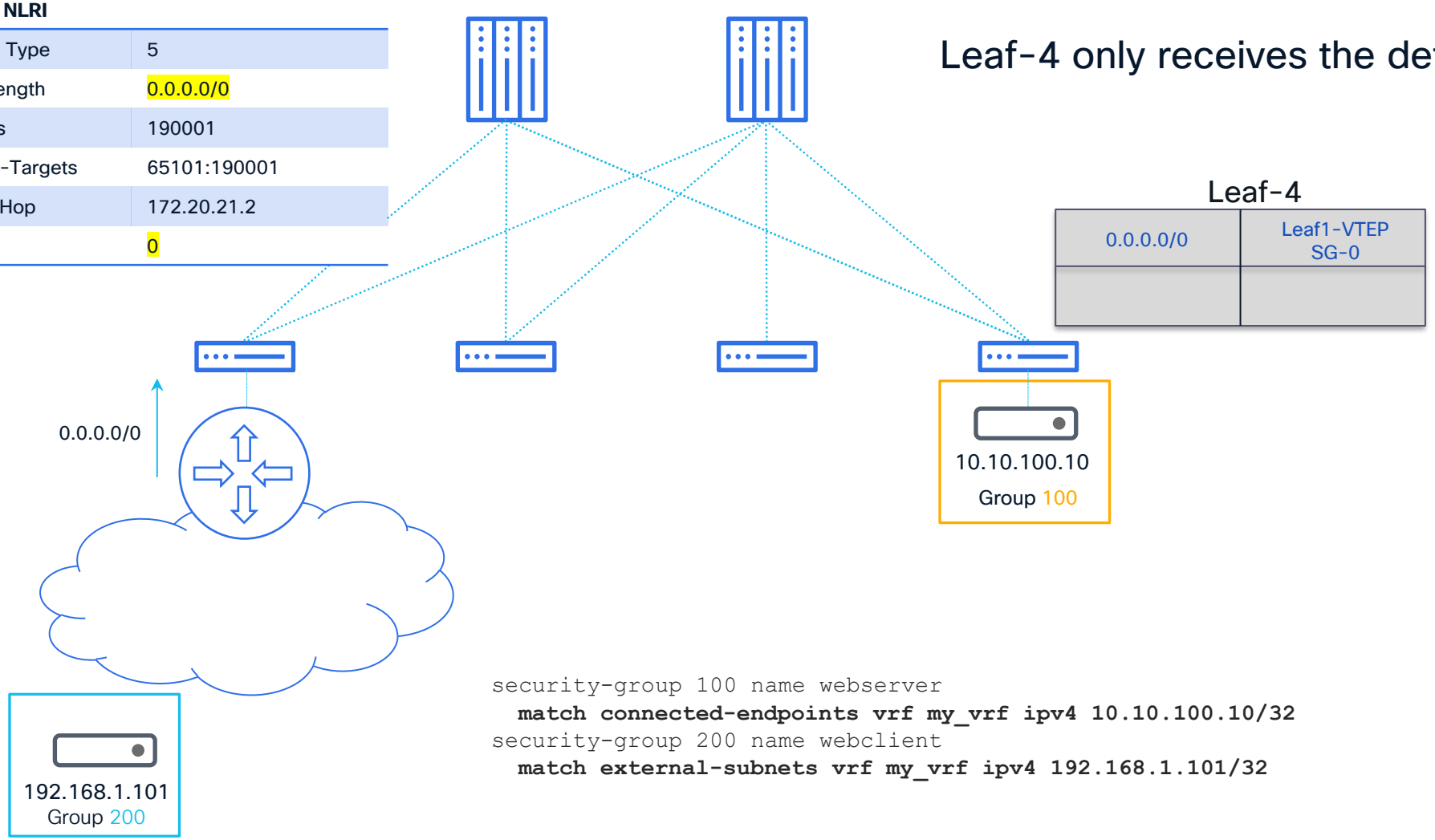
```
security-group 100 name webserver
  match connected-endpoints vrf my_vrf ipv4 10.10.100.10/32
security-group 200 name webclient
  match external-subnets vrf my_vrf ipv4 192.168.1.101/32
```

© 2025 Cisco and/or its affiliates. All rights reserved.

Group Policy Option Fundamentals

External Network Classifier – Broken Scenario

EVPN NLRI	
Route Type	5
IP / Length	0.0.0.0/0
Labels	190001
Route-Targets	65101:190001
Next-Hop	172.20.21.2
SGT	0



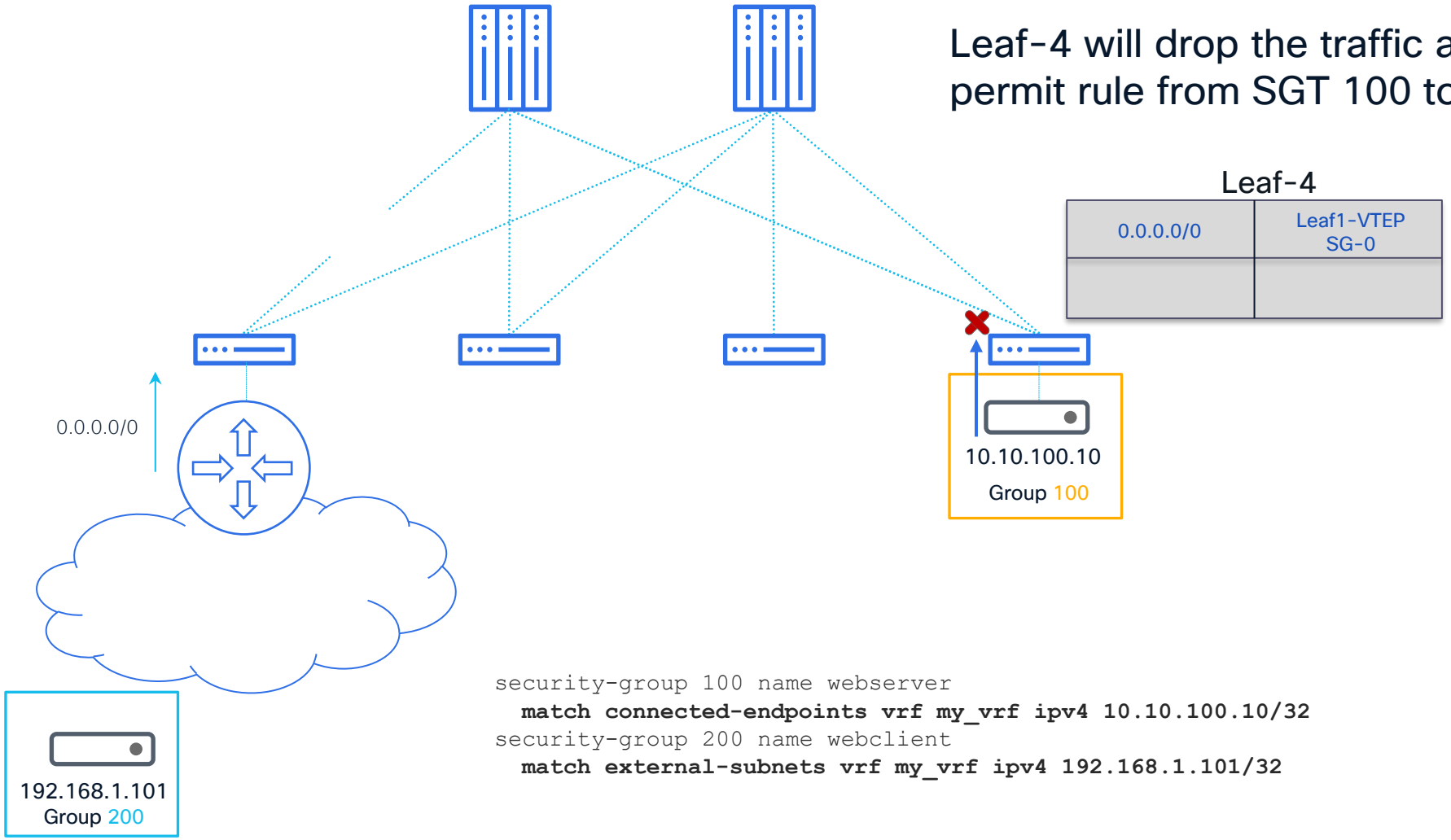
Leaf-4 only receives the default route with SGT 0

```
security-group 100 name webserver
  match connected-endpoints vrf my_vrf ipv4 10.10.100.10/32
security-group 200 name webclient
  match external-subnets vrf my_vrf ipv4 192.168.1.101/32
```

© 2025 Cisco and/or its affiliates. All rights reserved.

Group Policy Option Fundamentals

External Network Classifier – Broken Scenario



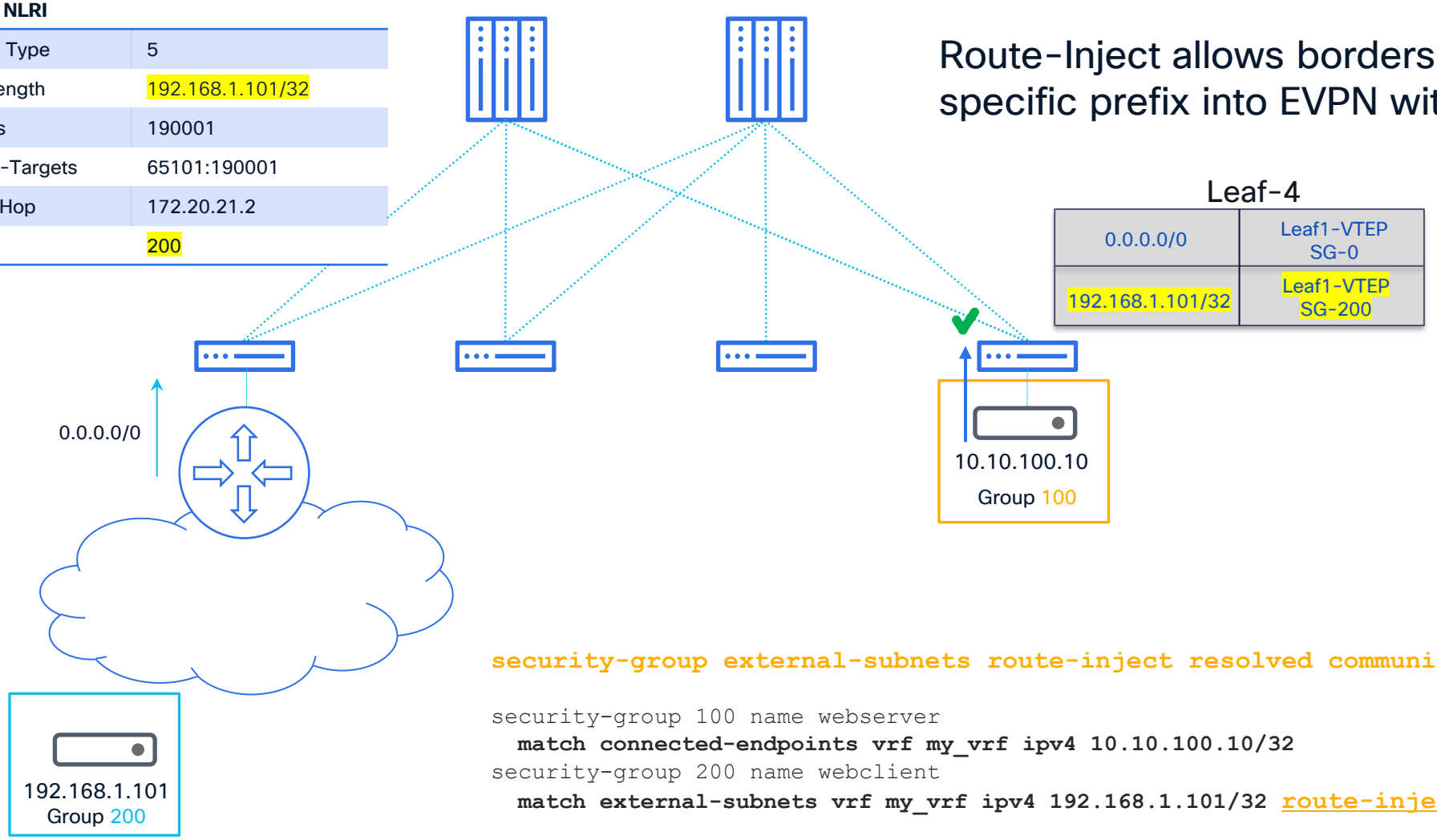

```
security-group 100 name webserver
  match connected-endpoints vrf my_vrf ipv4 10.10.100.10/32
security-group 200 name webclient
  match external-subnets vrf my_vrf ipv4 192.168.1.101/32
```

© 2025 Cisco and/or its affiliates. All rights reserved.

Group Policy Option Fundamentals

External Network Classifier – Route Inject to the Rescue!

EVPN NLRI	
Route Type	5
IP / Length	192.168.1.101/32
Labels	190001
Route-Targets	65101:190001
Next-Hop	172.20.21.2
SGT	200



Route-Inject allows borders to inject the more specific prefix into EVPN with the proper SGT

Leaf-4

0.0.0.0/0	Leaf1-VTEP SG-0
192.168.1.101/32	Leaf1-VTEP SG-200

```
security-group external-subnets route-inject resolved community 65101:999

security-group 100 name webserver
  match connected-endpoints vrf my_vrf ipv4 10.10.100.10/32
security-group 200 name webclient
  match external-subnets vrf my_vrf ipv4 192.168.1.101/32 route-inject
```

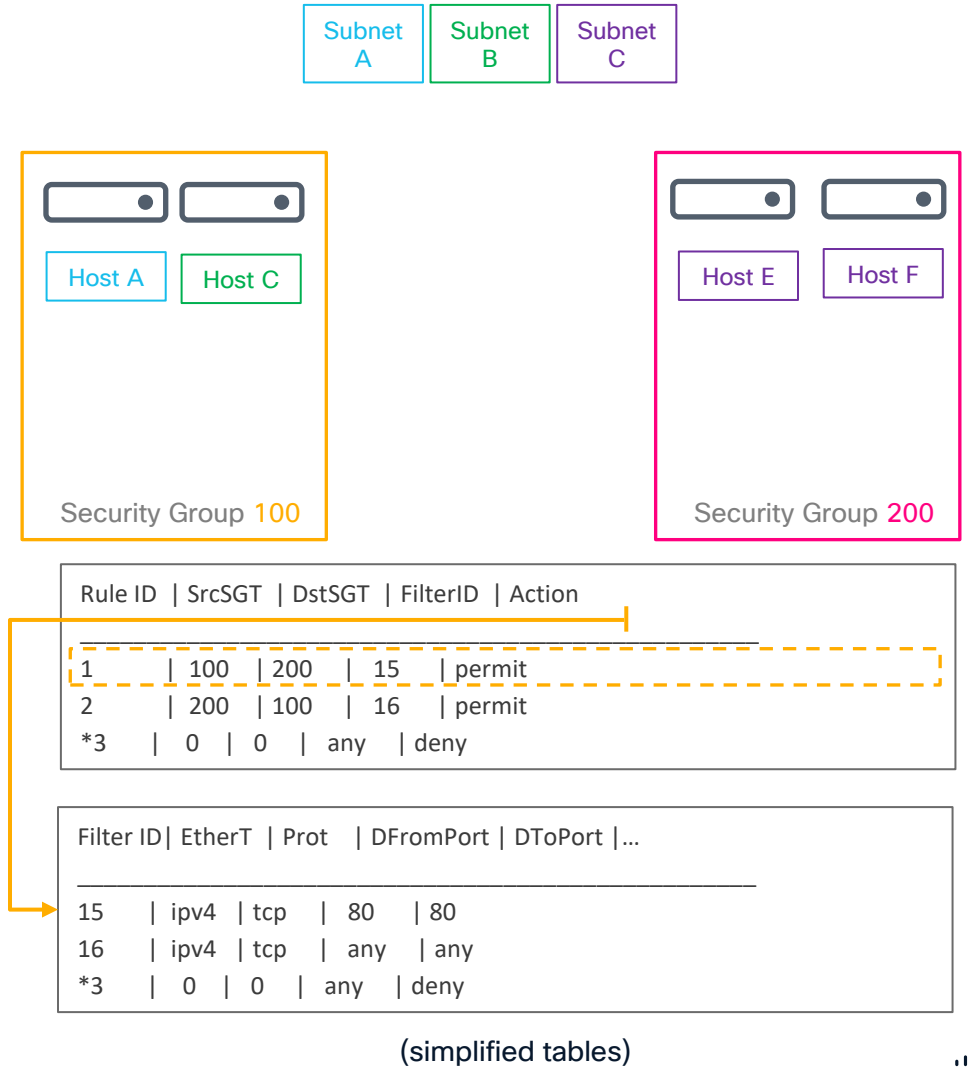
© 2025 Cisco and/or its affiliates. All rights reserved.

Group Policy Option Fundamentals

**Hidden Slide Follows

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)

© 2025 Cisco and/or its affiliates. All rights reserved.

Group Policy Option Fundamentals

Traffic Enforcement – Contract priorities – Base Rules

In case of a ties the following logics will be used

1. Specific SGs win over Any
   i. SG-100 to SG-200
   ii. SG-100 to Any
   iii. Any to SG-100
   iv. Any to Any
2. More specific protocol rule win
   i. tcp.dst 80
   ii. tcp.src 80
   iii. tcp.any
   iv. IP
3. Action priority
   i. Deny
   ii. Redirect
   iii. Permit

© 2025 Cisco and/or its affiliates. All rights reserved.

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
```

© 2025 Cisco and/or its affiliates. All rights reserved.

Group Policy Option Fundamentals

Traffic Enforcement – Policies

- Policies, or contracts/SG-ACLs, define the action that will be programmed on the hardware (filter):
  - Permit
  - Deny
  - Redirect to a Service function (or a *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

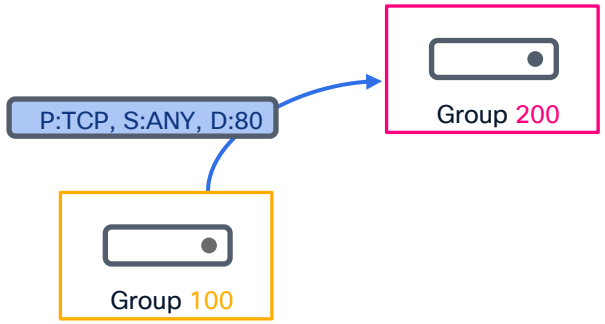
```
policy-map type security VPN-CLIENTS-TO-ANY
 class TCP-PORT-80
  log
  service-chain WEB-CHAIN-SITE-1
 class MANAGEMENT
  permit
 class default
  log
  deny

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

© 2025 Cisco and/or its affiliates. All rights reserved.

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



vrf context my_vrf

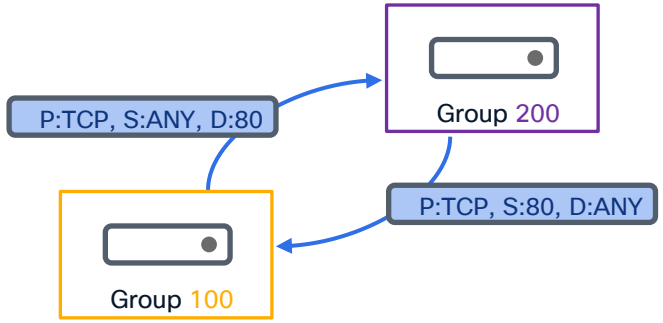
security contract source 100 destination 200 policy ONLY-TCP-PORT-80 unidir

© 2025 Cisco and/or its affiliates. All rights reserved.

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*
```

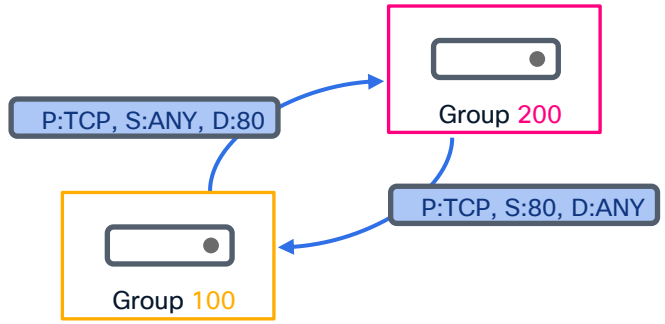
*default setting

© 2025 Cisco and/or its affiliates. All rights reserved.

Group Policy Option Fundamentals

Traffic Enforcement – Stateful Filters and Bidirectional Rules

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

policy-map type security CLIENTS-TO-WEB
  class TCP-PORT-80
  permit

vrf context my_vrf
  security contract source 100 destination 200 policy CLIENTS-TO-WEB bidir
```

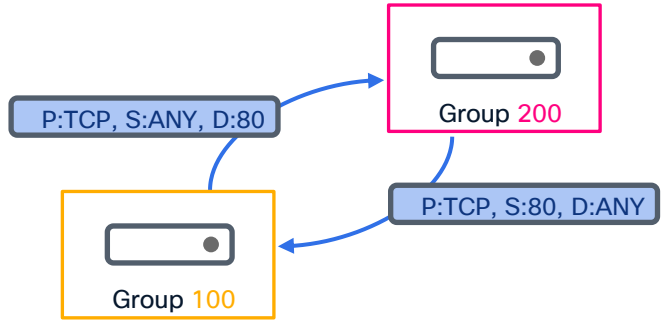


© 2025 Cisco and/or its affiliates. All rights reserved.

Group Policy Option Fundamentals

Traffic Enforcement – Stateful Filters and Bidirectional Rules

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

policy-map type security CLIENTS-TO-WEB
  class TCP-PORT-80
  permit

vrf context my_vrf
  security contract source 100 destination 200 policy CLIENTS-TO-WEB bidir
```



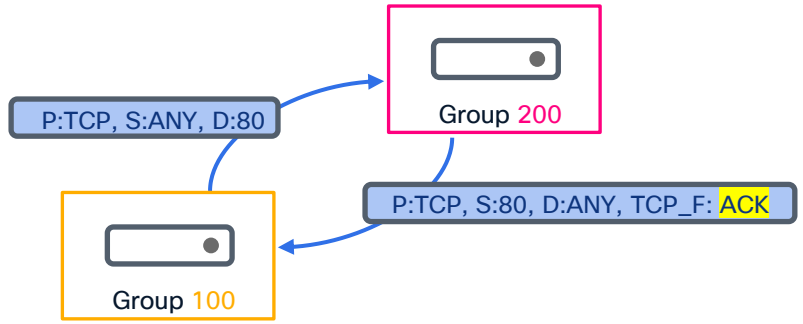
Non Expected Traffic

© 2025 Cisco and/or its affiliates. All rights reserved.

Group Policy Option Fundamentals

Traffic Enforcement – Stateful Filters and Bidirectional Rules

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

policy-map type security CLIENTS-TO-WEB
  class TCP-PORT-80
  permit

vrf context my_vrf
  security contract source 100 destination 200 policy CLIENTS-TO-WEB bidir
```

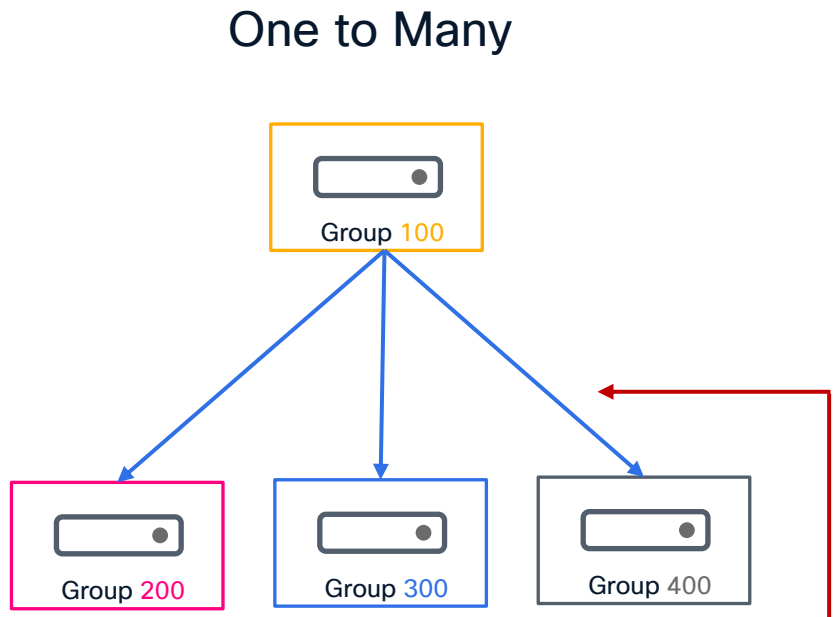


© 2025 Cisco and/or its affiliates. All rights reserved.

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



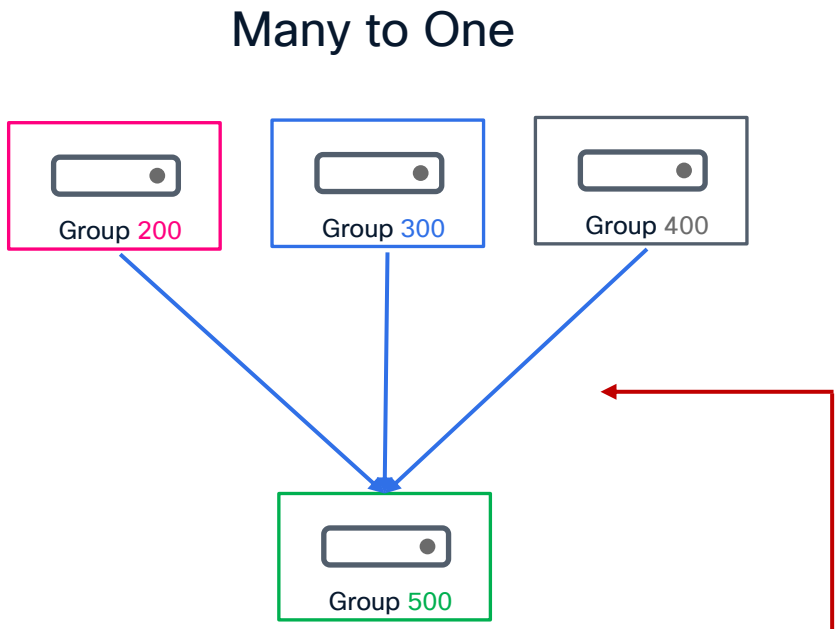

```
vrf context my_vrf
  security con sou 100 dest any policy MANAGEMENT bidir
  security con sou any dest 500 policy BACKUP bidir
  security con sou any dest any policy FIREWALL-REDIRECTION bidir
```

© 2025 Cisco and/or its affiliates. All rights reserved.

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



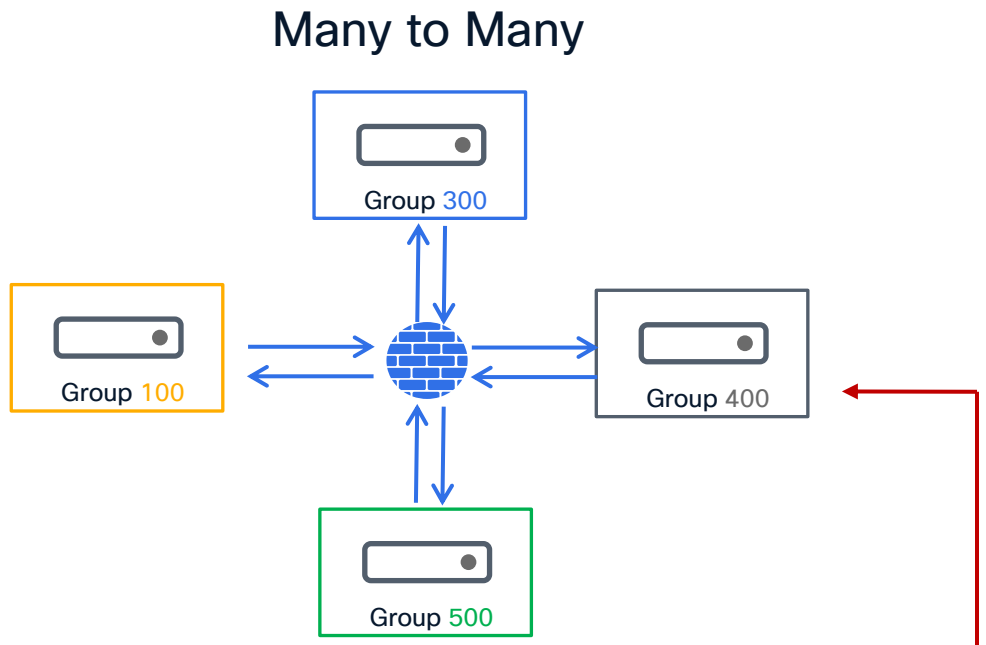

```
vrf context my_vrf
  security con sou 100 dest any policy MANAGEMENT bidir
  security con sou any dest 500 policy BACKUP bidir
  security con sou any dest any policy FIREWALL-REDIRECTION bidir
```

© 2025 Cisco and/or its affiliates. All rights reserved.

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



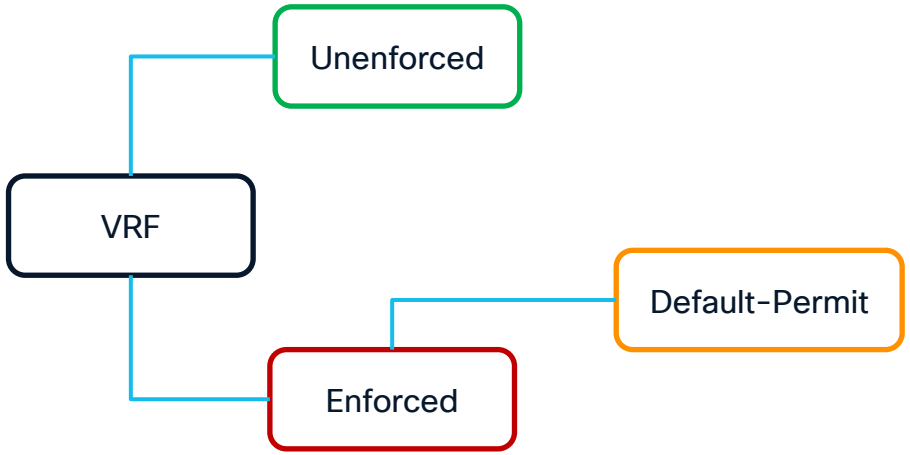

```
vrf context my_vrf
  security con sou 100 dest any policy MANAGEMENT bidir
  security con sou any dest 500 policy BACKUP bidir
  security con sou any dest any policy FIREWALL-REDIRECTION bidir
```

© 2025 Cisco and/or its affiliates. All rights reserved.

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



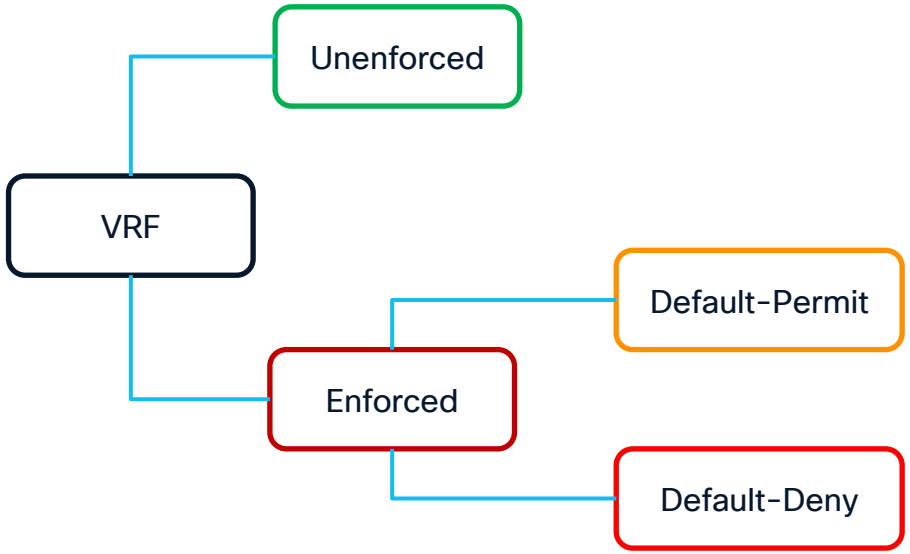

```
vrf context my_vrf
  security enforce tag 13129 default permit
```

© 2025 Cisco and/or its affiliates. All rights reserved.

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

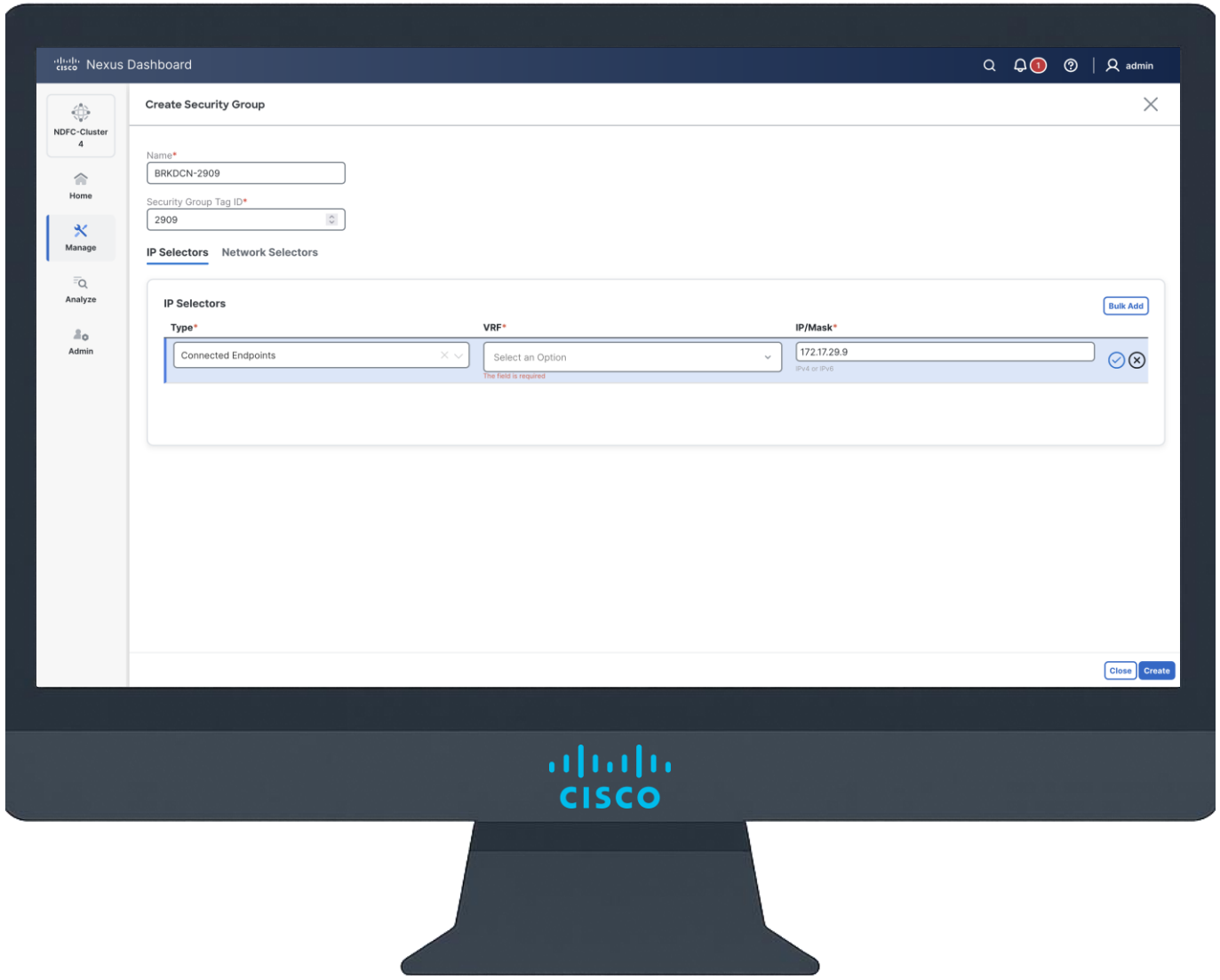



```
vrf context my_vrf
  security enforce tag 13129 default deny
```

© 2025 Cisco and/or its affiliates. All rights reserved.

Group Policy Option Fundamentals

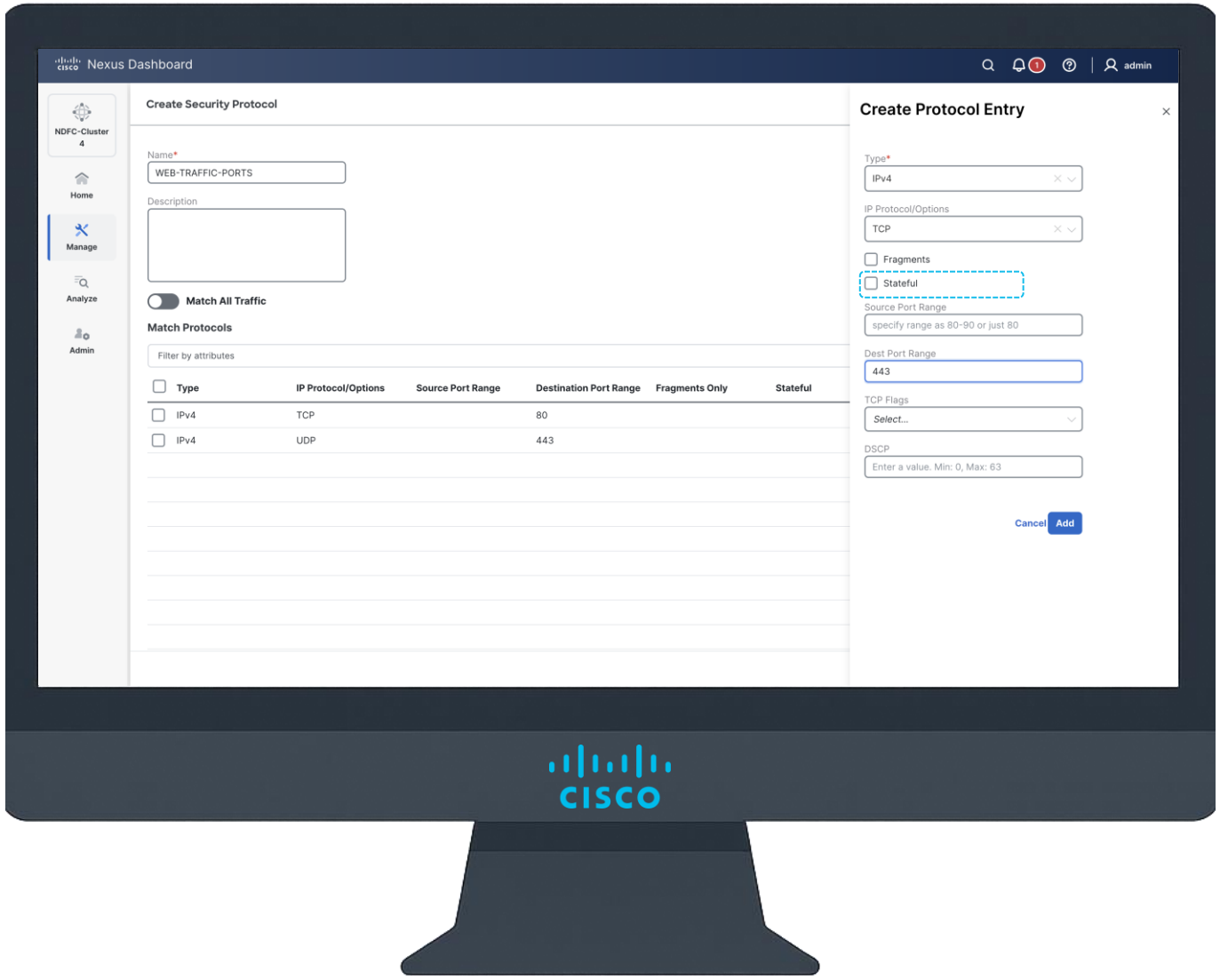
Nexus Dashboard Security Groups



© 2025 Cisco and/or its affiliates. All rights reserved.

Group Policy Option Fundamentals

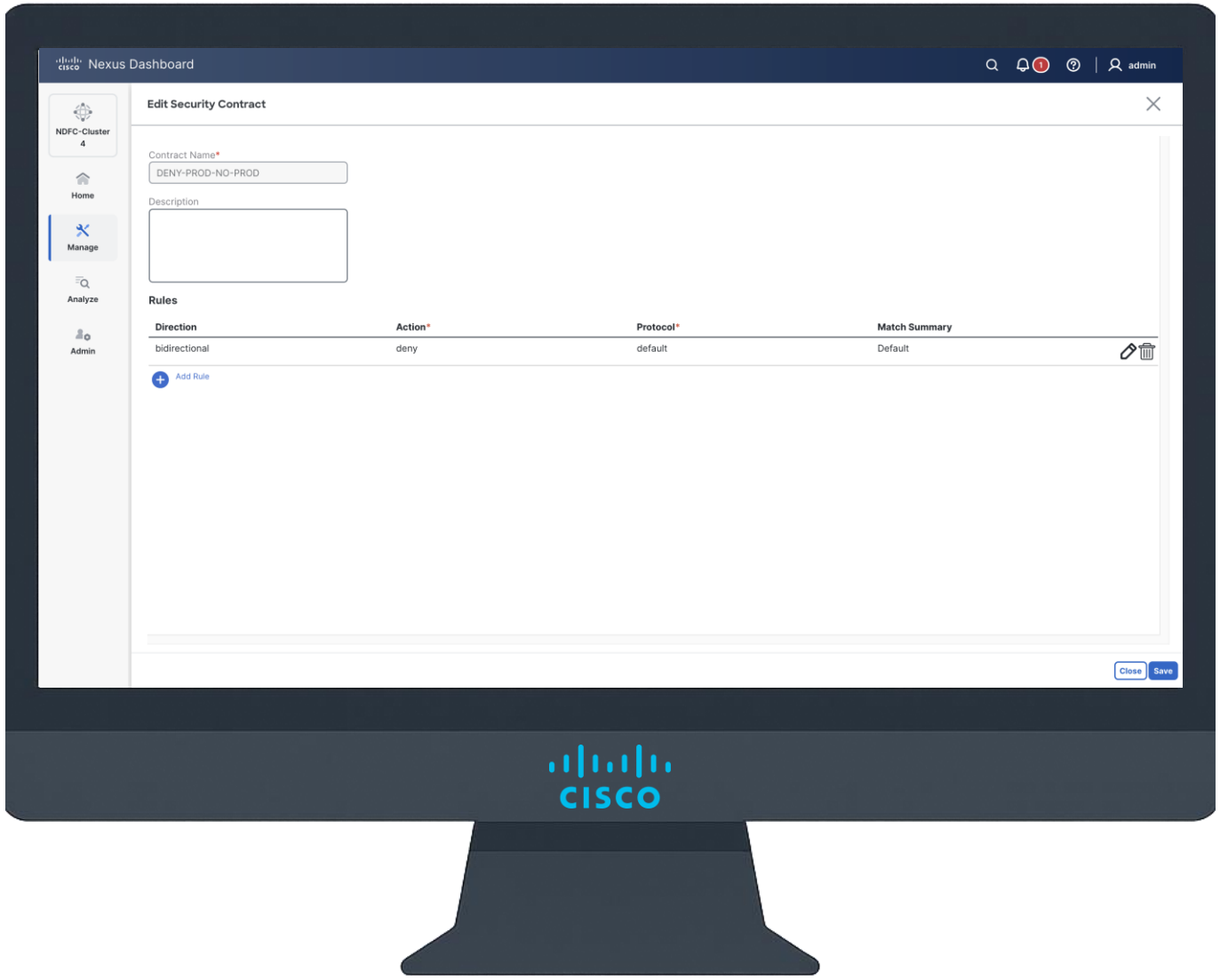
Nexus Dashboard Security Protocols



© 2025 Cisco and/or its affiliates. All rights reserved.

Group Policy Option Fundamentals

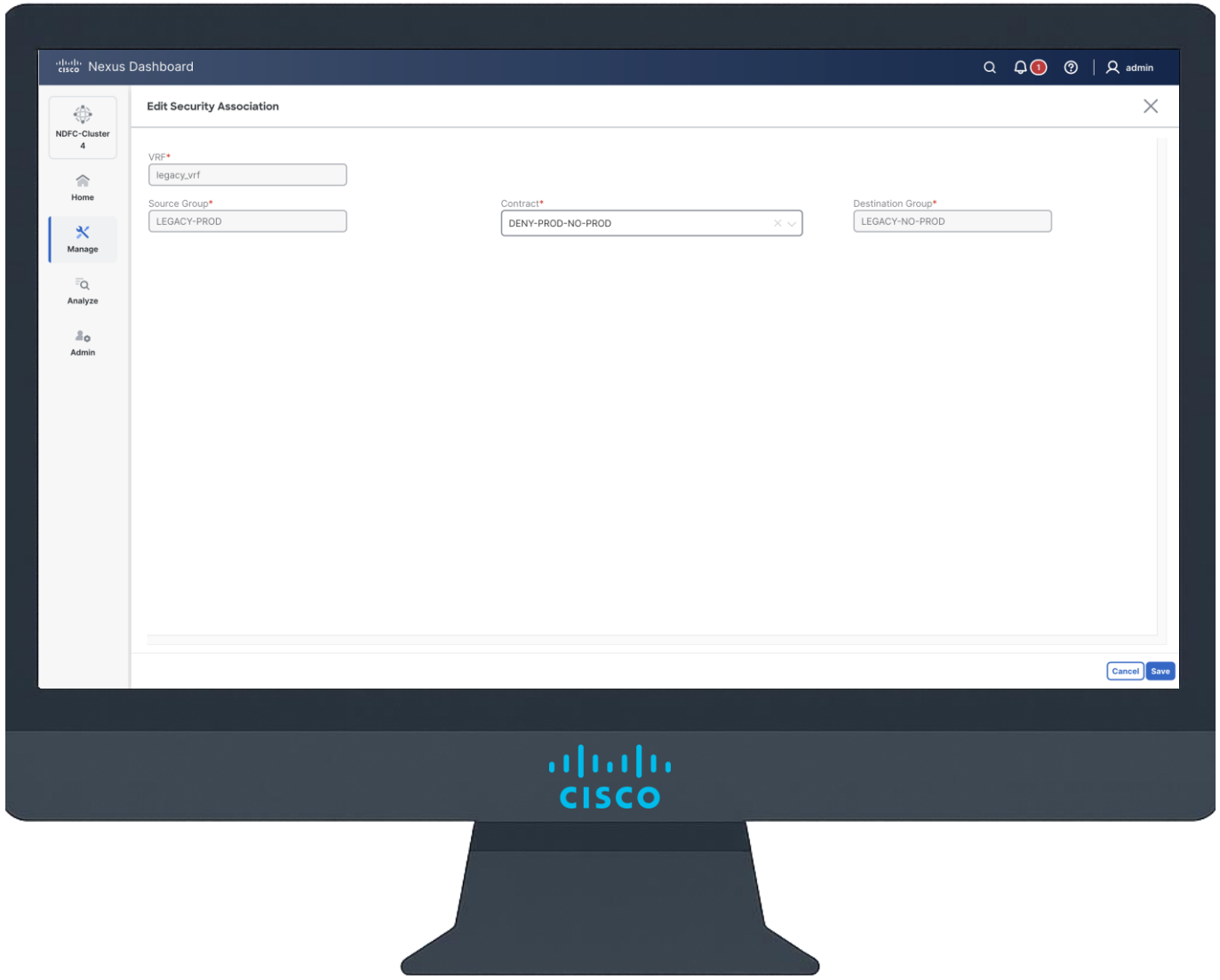
Nexus Dashboard Contracts



© 2025 Cisco and/or its affiliates. All rights reserved.

Group Policy Option Fundamentals

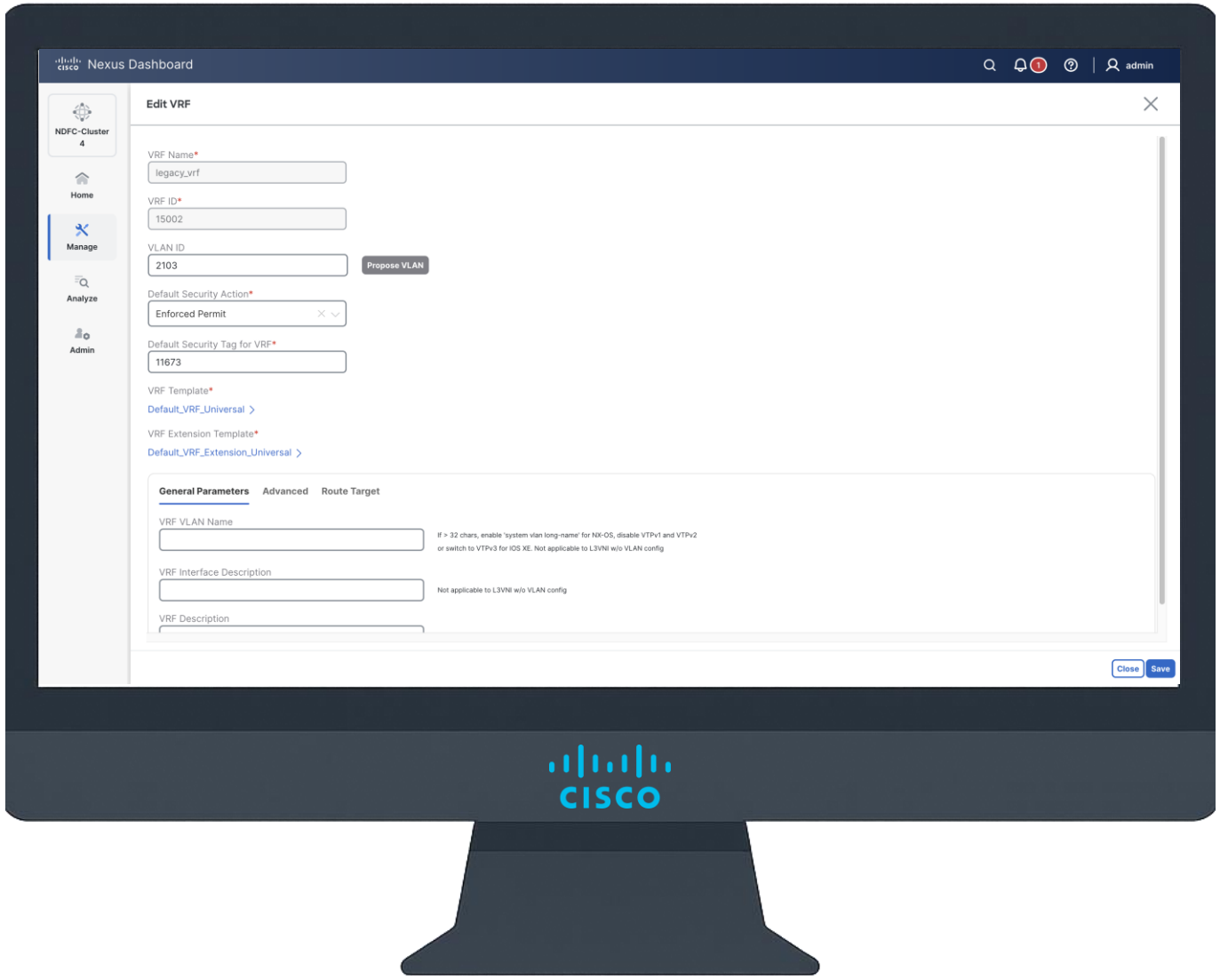
Nexus Dashboard Associations



© 2025 Cisco and/or its affiliates. All rights reserved.

Group Policy Option Fundamentals

Nexus Dashboard VRF Settings



© 2025 Cisco and/or its affiliates. All rights reserved.

Demo #1

GPO Based Service Redirection

Service Insertion

What is it and Why do we need it?

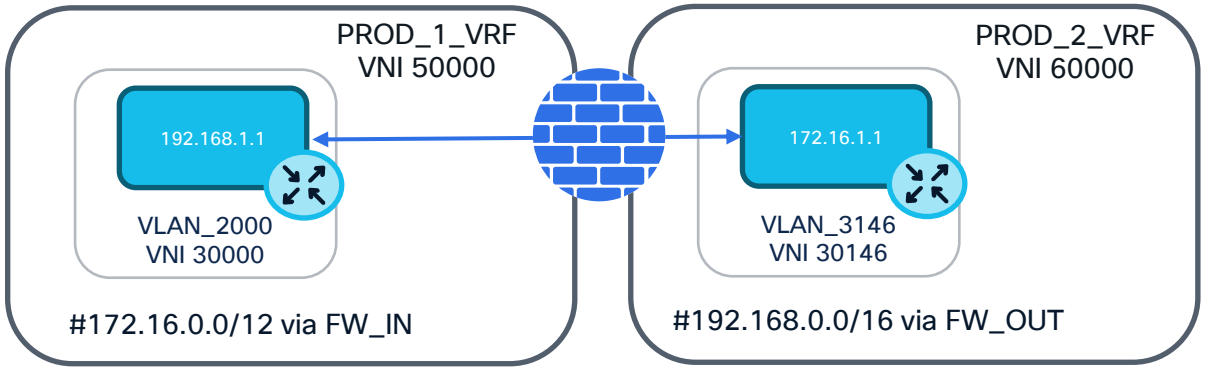
- Offload the traffic to a device connected to the fabric for additional processing
- Stateless ACLs might not be enough
- Companies' security policies might require advance traffic policies for some or all the traffic
- Security teams want to own the devices and the policies that inspect the traffic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

© 2025 Cisco and/or its affiliates. All rights reserved.

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
  - Distributed Anycast Gateway (DAG) when firewall is used as default gateway
  - VRF Leaking with the perimeter firewall



Classic VRF Sandwich

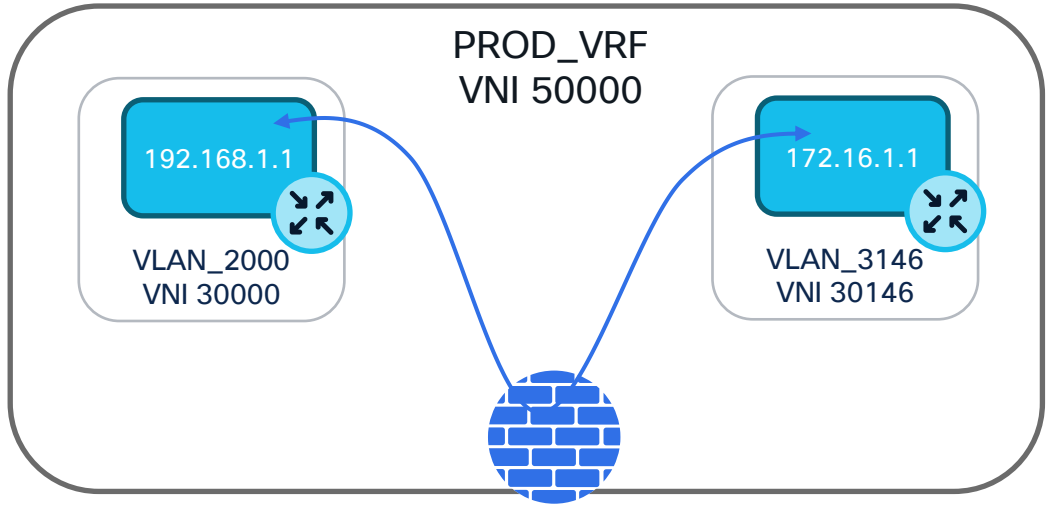
https://www.cisco.com/c/en/us/td/docs/dcn/whitepapers/cisco-vxlan-multi-site-and-service-node-integration.html

© 2025 Cisco and/or its affiliates. All rights reserved.

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
- 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 with IP SLA
  - Supports IP access-list and now GPO

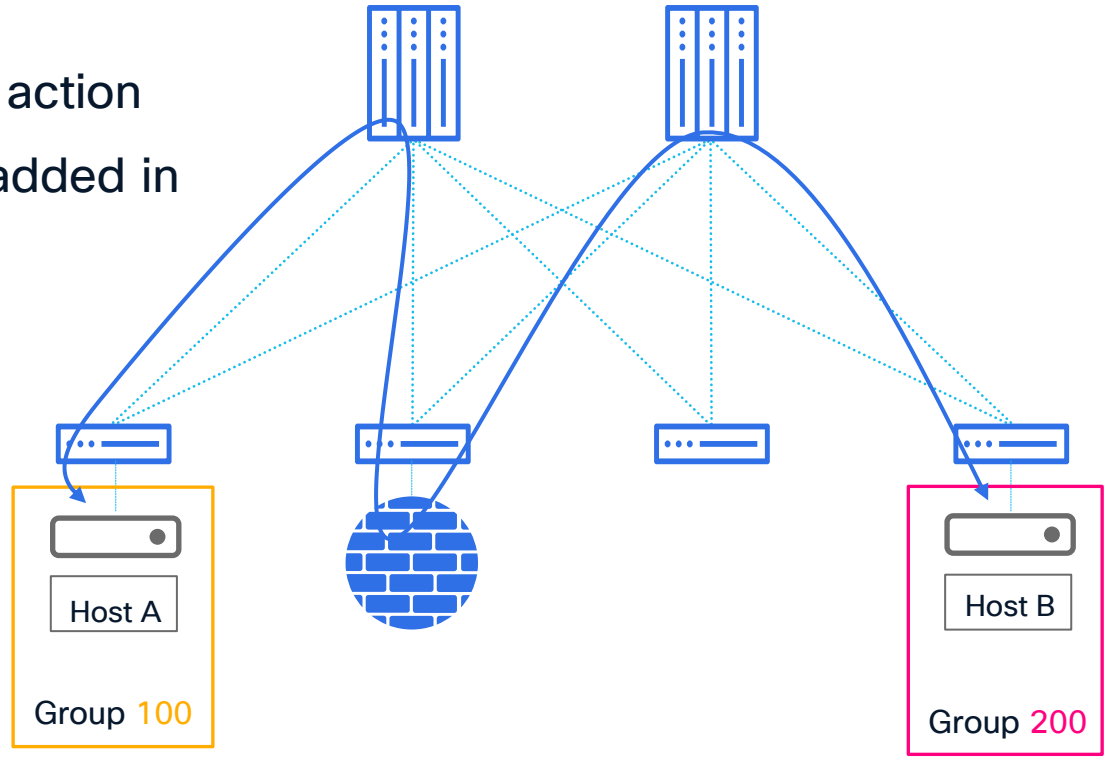


© 2025 Cisco and/or its affiliates. All rights reserved.

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
- Redirection can happen for specific traffic flows
  - Granular match rules (filters)
- Not yet available in Nexus Dashboard (ND)
  - A workaround will be explored in the next demo

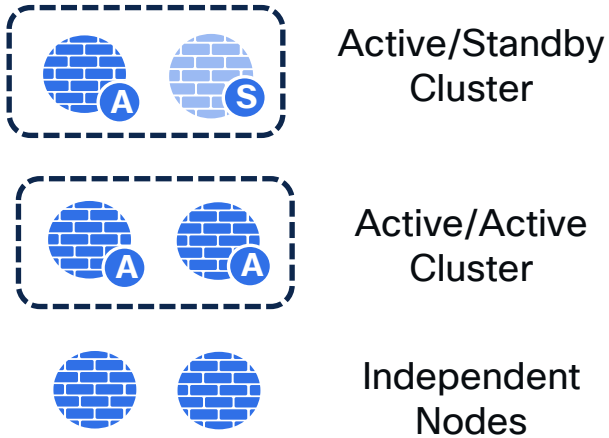


© 2025 Cisco and/or its affiliates. All rights reserved.

GPO Based Service Redirection

Terminology

Service Endpoint



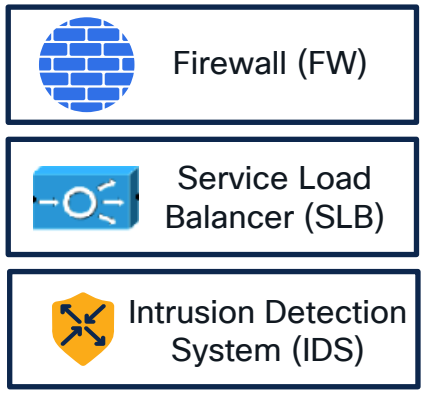
Active/Standby Cluster

Active/Active Cluster

Independent Nodes

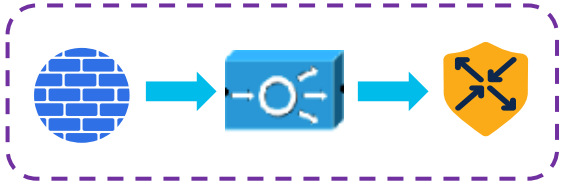
- Physical or virtual devices that handle the received traffic flows
- Can be deployed with different redundancy models (Active/Active, Active/Standby, Independent Nodes)

Service Function



- An entity that includes one or multiple service endpoints (service devices)
- Service devices of the same type implement the same logical function

Service-Chain



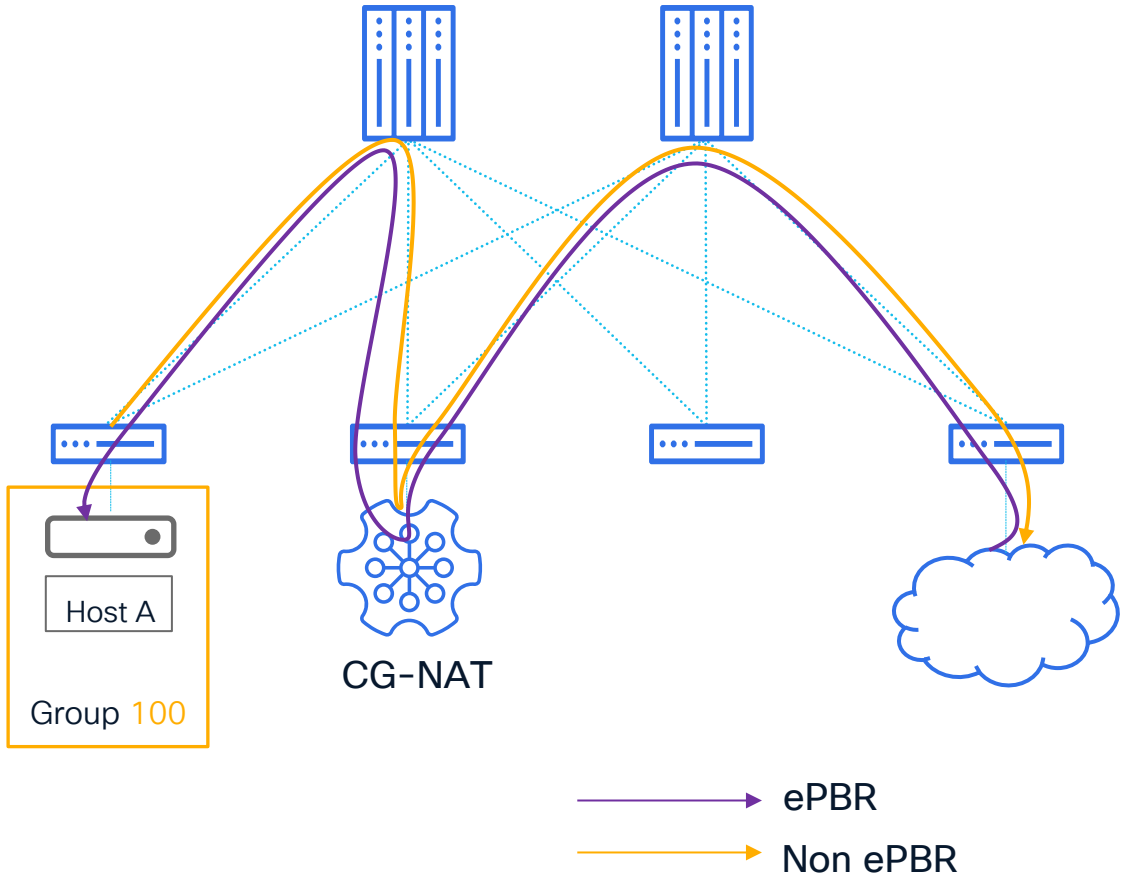
- A group of ordered Service Functions that traffic flows will need to traverse
- Service-chain configuration provides options to test the reachability and eventually skip a failed function

© 2025 Cisco and/or its affiliates. All rights reserved.

GPO Based Service Redirection

Service Endpoint

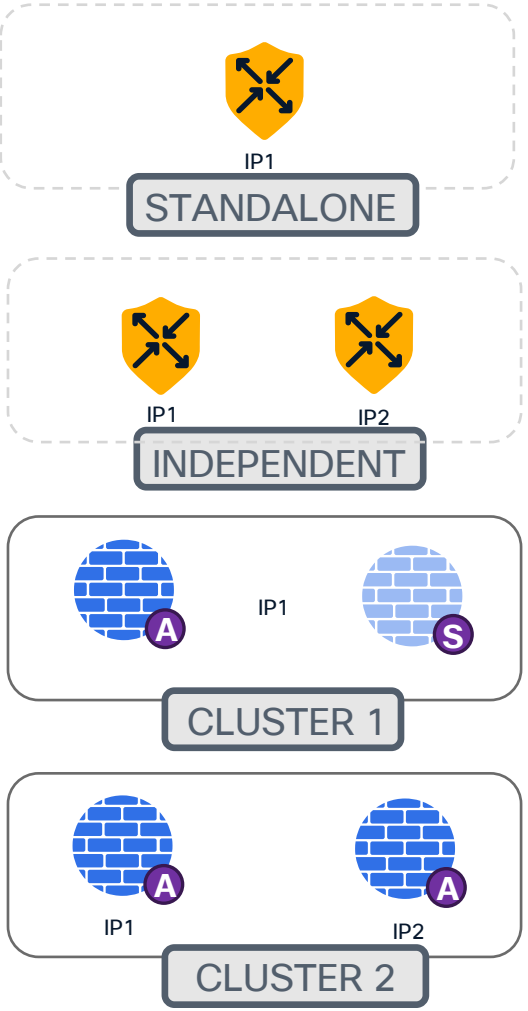
- Service Endpoints are networking devices that apply additional policies to the traffic
  - They can be Virtual or Physical
  - They can be standalone or deployed in clusters
- Depending on their function they might required different redirection rules
  - Device that do not apply any NAT rules like 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



© 2025 Cisco and/or its affiliates. All rights reserved.

GPO Based Service Redirection

Service Endpoints and Service Functions



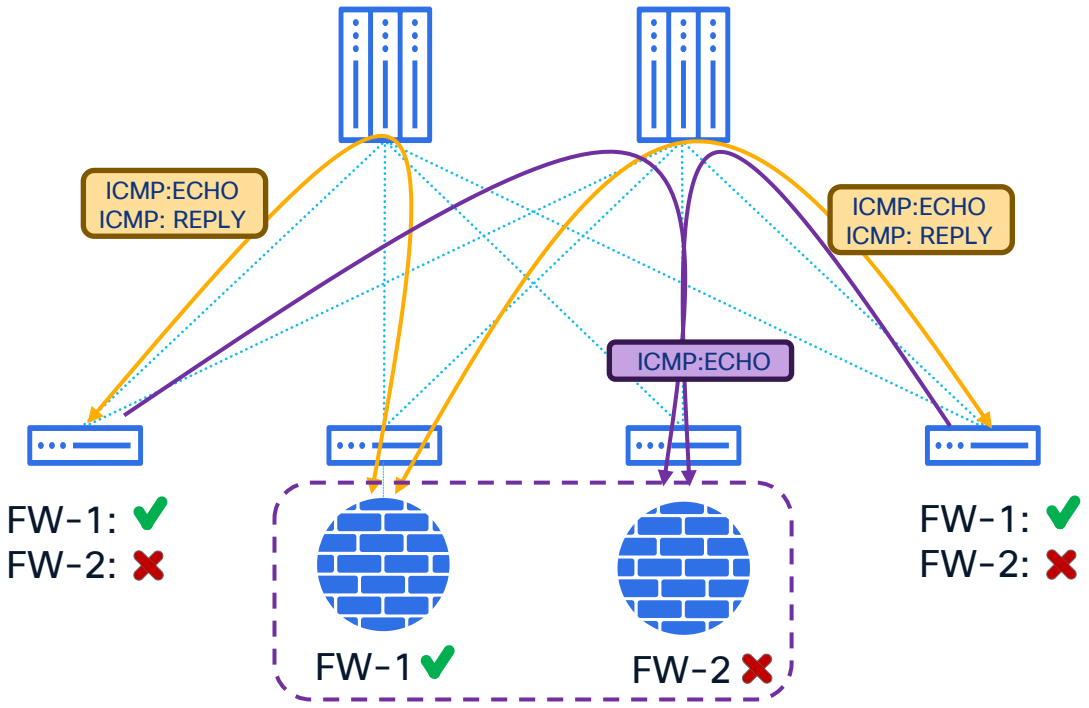
- Service Functions are logical groups of Service-Endpoints that enforce the same traffic policies
- Service Functions can contain one or multiple service endpoints
- They can be used to set the IP SLA monitoring, and they will take the device in and out of the pool based on their status
- Service endpoints implementing a specific Service Function must be classified in one (or more) ESGs

```
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
```

© 2025 Cisco and/or its affiliates. All rights reserved.

GPO Based Service Redirection

Service Function - Tracking



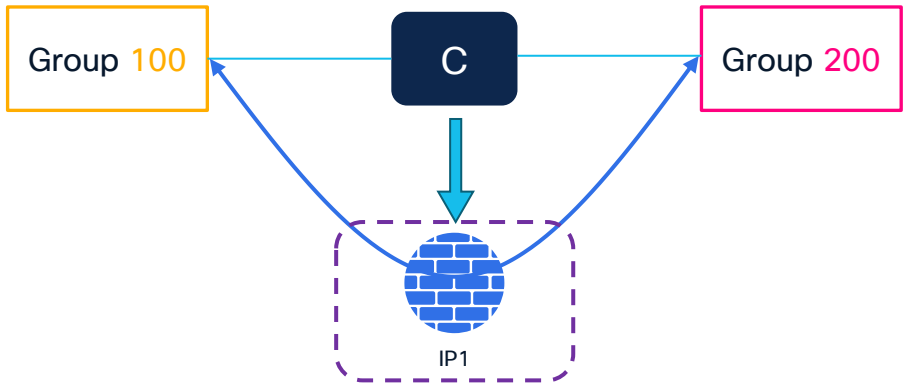
- Tracking the health of devices avoids blackholes
- All the VTEPs where the traffic is forwarded needs to track the status of the devices via loopbacks
- Unhealthy Service Endpoints must be excluded from the Service Function pool
- Probes can be configured with different protocols
  - ICMP, UDP, TCP, HTTP, DNS

```
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
```

© 2025 Cisco and/or its affiliates. All rights reserved.

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

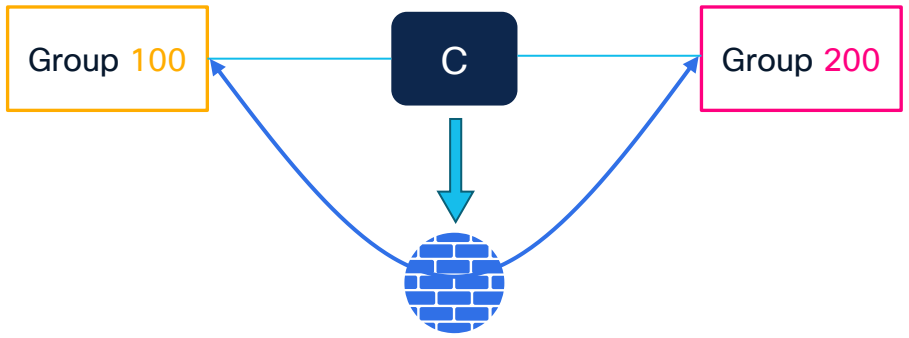
10 set service FIREWALL-1-SITE-1

action redirect

© 2025 Cisco and/or its affiliates. All rights reserved.

GPO Based Service Redirection

Service Chains - Single Function



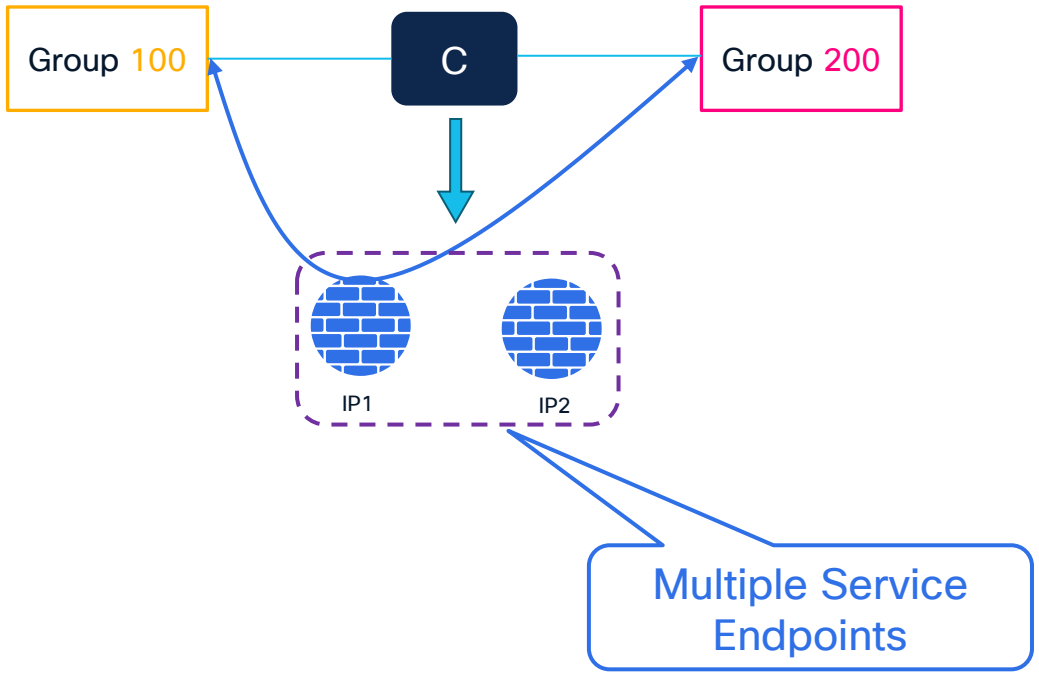
- Service Chains allow us to define the traffic redirection rules
- When traffic is redirected to a service-chain it needs to cross all the functions listed there.
  - If a function is not UP, we can decide the action
    - Forward – Send the packet to the destination IP
    - Drop – Discard the packet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

```
epbr service-chain WEB-CHAIN-SITE-1
 10 set service FIREWALL-1-SITE-1 fail-action drop
  action redirect
```

© 2025 Cisco and/or its affiliates. All rights reserved.

GPO Based Service Redirection

Service Chains - Single Function

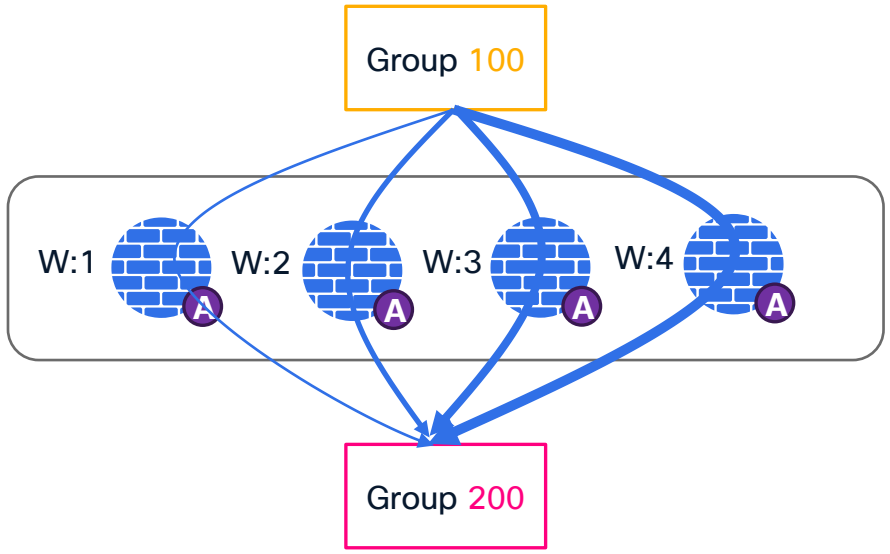


- Multiple Service Endpoints for a function can be deployed in different ways
  - Cluster: Active/Active (cluster members with individual IPs)
  - Independent devices with synchronized policies
- Symmetry is always maintained
  - When multiple service endpoints, with different IP addresses, are defined inside a function, traffic in both directions is always sent to the same node (symmetric service redirection)

© 2025 Cisco and/or its affiliates. All rights reserved.

GPO Based Service Redirection

Service Chains – Load Balancing for a Single Function



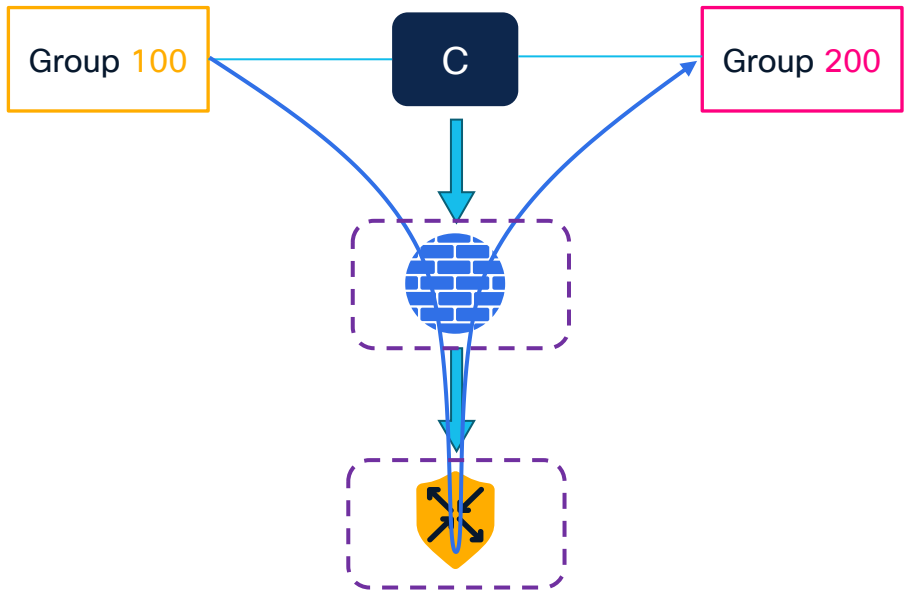

```
epbr service-chain SINGLE-FUNCT-CHAIN-SITE-1
 load-balance method src-dst-ipprotocol
 10 set service FIREWALL-1-SITE-2 fail-action drop
  load-balance method dst-ip
```

- Load Balancing is used when multiple Service Endpoints build a given Service Function
- Load Balancing hash might be calculated based on:
  - Source IP Address
  - Destination IP Address
  - Source, Destination IP Addresses and IP Protocol
  - Global configuration for the whole service-chain with possible override at the service function level
- Load Balancing uses resilient hashing
  - When a device fails, only the flows that were hashed to it will be re-hashed. The same happens when device comes back in the pool
- Two optional methods can be used and combined:
  - Weighted Load Balancing: unequally distributes the load over the different service endpoints
  - N+M Redundancy: Hot Standby devices ready to takeover the failed one(s)

© 2025 Cisco and/or its affiliates. All rights reserved.

GPO Based Service Redirection

Service Chains – Multi Function



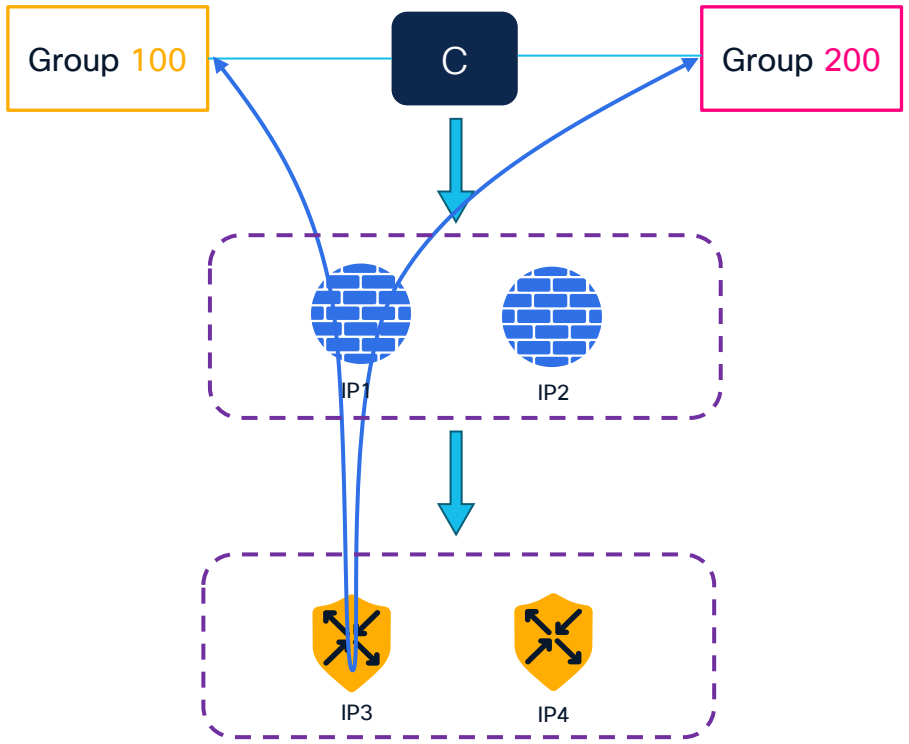
- Service Chains can contain multiple functions
- Each function is mapped to a sequence number that sets the order
  - Returning traffic will follow the order backwords
- If a function is not UP, we can decide the action
  - ~~Forward~~ – (cannot be used with multi function service-chains)
  - Drop –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

```
epbr service-chain WEB-CHAIN-SITE-1
 10 set service FIREWALL-1-SITE-1 fail-action bypass
   action redirect
 20 set service IDS-1-SITE-1 fail-action drop
   action redirect
```

© 2025 Cisco and/or its affiliates. All rights reserved.

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
```

© 2025 Cisco and/or its affiliates. All rights reserved.

GPO Based Service Redirection

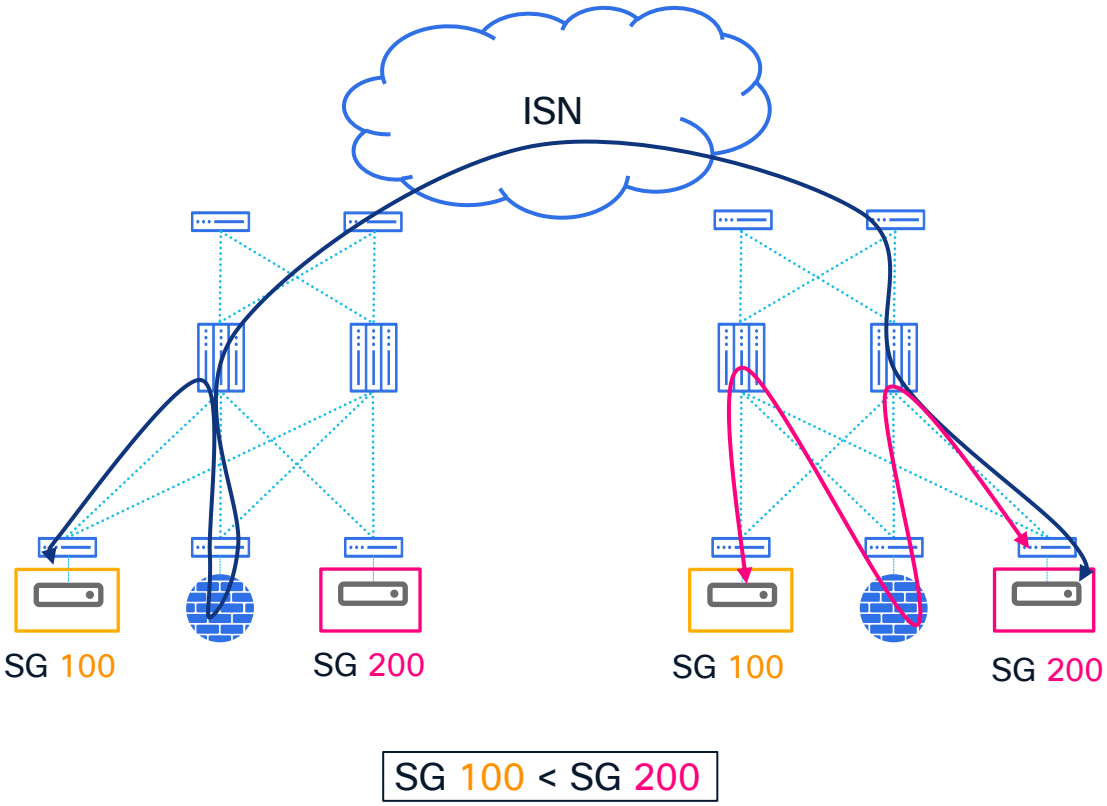
Multi-Site Highlights

- Multi-Site support added in NX-OS 10.5(2)F
- Works with single an multi function Service Chains
- Traffic hair-pinning is kept minimal in normal conditions
- Symmetry is always maintained, ensuring traffic returns to the same service cluster
  - Traffic can be intra-site; in this case the local Service Chain is used; Assuming that there is a local SC.
  - Traffic can be inter-site; in this case we will use a deterministic algorithm to pick the same chain for both direction
- Works when a site has no local Service Endpoints by design
  - Always consider the latency increase when redirecting to a different site
- All Service Endpoints in a Service Chain must be attached to the same site. **Mandatory!**
- If a function fails, the entire service-chain is considered as failed, the **failover-group** will be used
  - If the fail-action of the function is bypass, the above rule is relaxed

© 2025 Cisco and/or its affiliates. All rights reserved.

GPO Based Service Redirection

Multi-Site Highlights

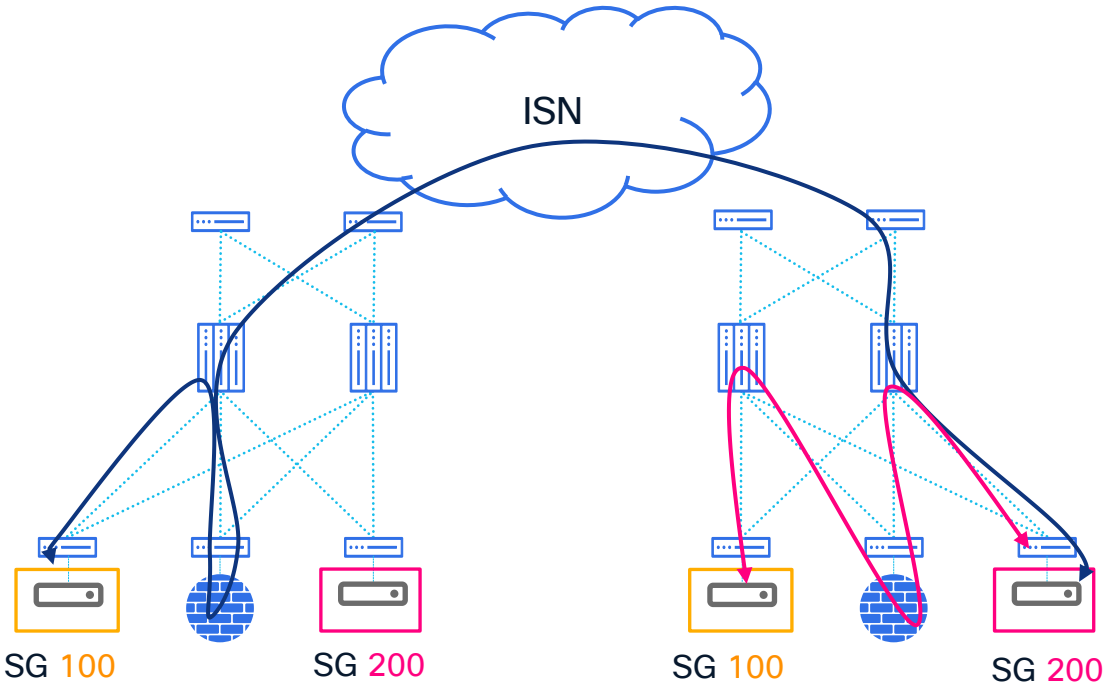


- Multi-Site support added in NX-OS release 10.5(2)F
- Works with single and multi functions Service Chains
- Traffic hair-pinning is kept to minimal in normal conditions
- Symmetry is always maintained, ensuring traffic returns to the same service cluster
  - Traffic can be intra-site: in this case the local Service Chain is used (assuming that a local chain is present)
  - Traffic can be inter-site: in this case we will use a deterministic algorithm to pick the same chain for both direction

© 2025 Cisco and/or its affiliates. All rights reserved.

GPO Based Service Redirection

Keeping Intersite Redirection Symmetric

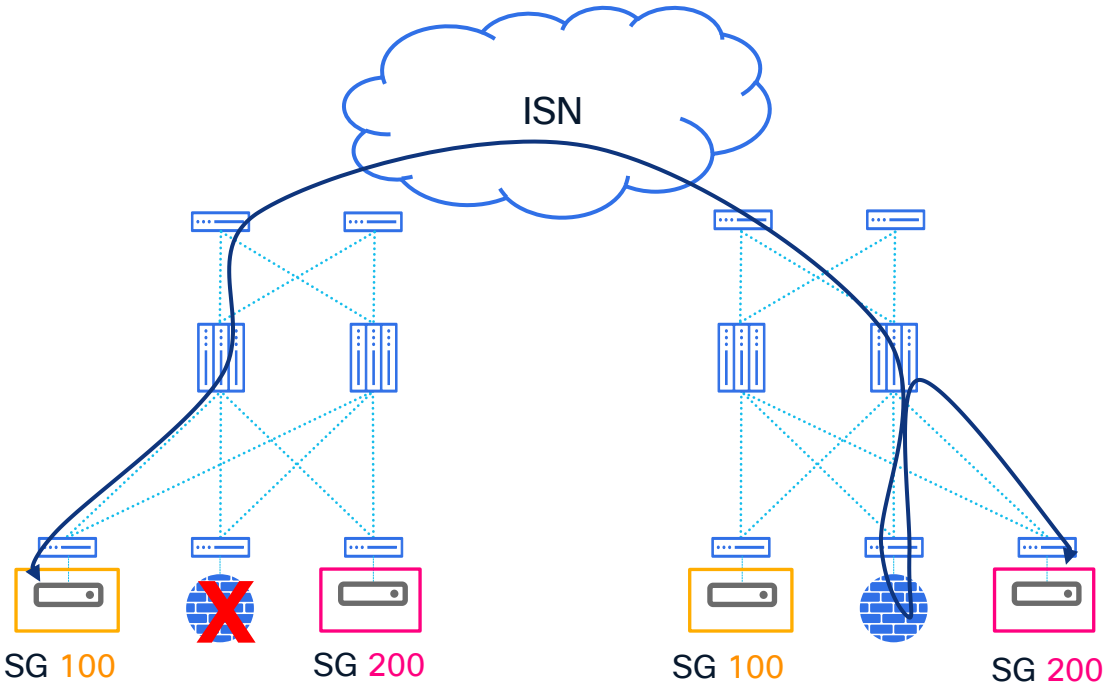


- Symmetricity in Service Chains is achieved by ensuring that data traffic use the Service Chain at either the source or destination site, known as site pinning
- If the Source Security Group Tag (S-SGT) is lower than the Destination Security Group Tag (D-SGT), VTEPs sends the traffic to local Service-Chain, provided it is operational
- Otherwise, VTEPs take in account the destination EP locality:
  - If destination EP is local then traffic is sent to the preferred Service-Chain, provided it is operational. At the end this must be considered intra-site traffic
  - If destination EP is remote, then traffic is forwarded by a permit rule towards the destination site. The first VTEP in the destination site (the BGW) will apply the redirect and send it to the preferred Service-Chain, provided it is operational

© 2025 Cisco and/or its affiliates. All rights reserved.

GPO Based Service Redirection

Keeping Intersite Redirection Symmetric



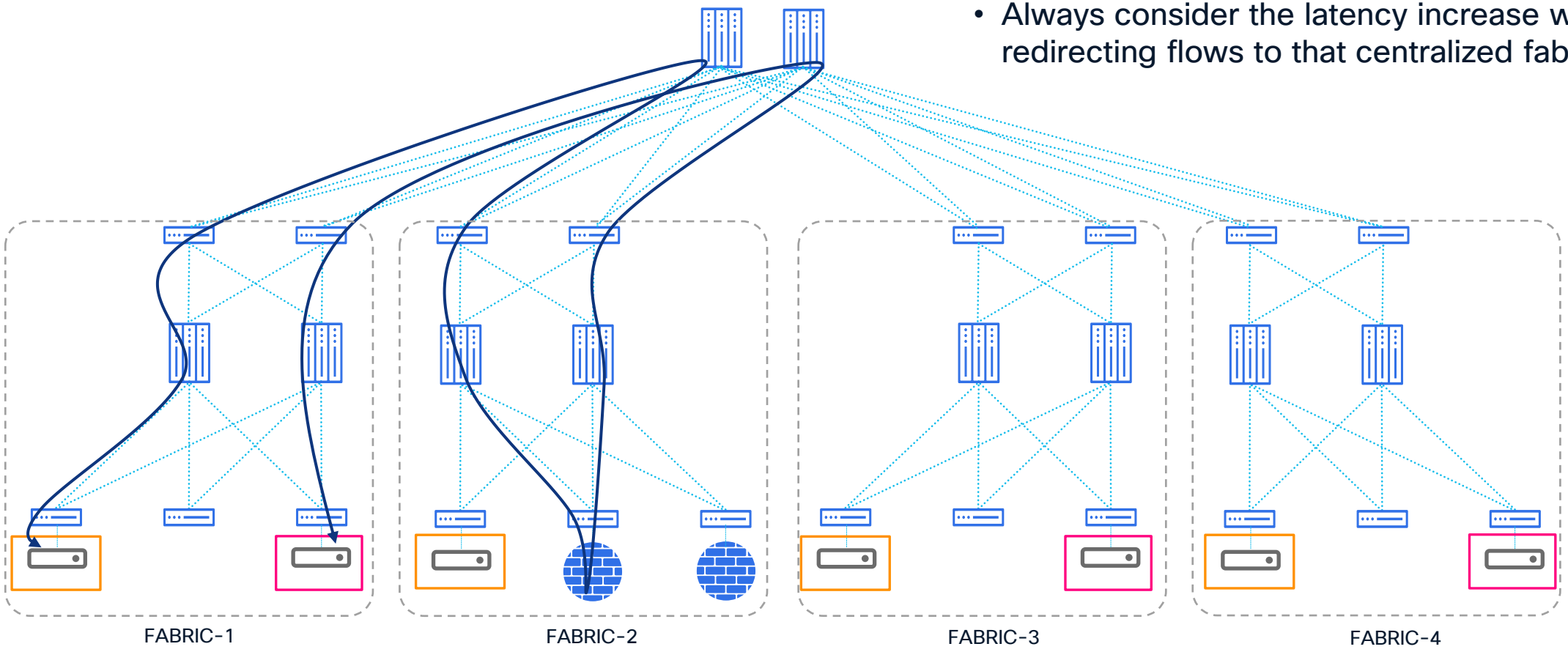
- Symmetricity in Service Chains is achieved by ensuring that data traffic use the Service Chain at either the source or destination site, known as site pinning
- If the Source Security Group Tag (S-SGT) is lower than the Destination Security Group Tag (D-SGT), VTEPs sends the traffic to local Service-Chain, provided it is operational
- Otherwise, VTEPs take in account the destination EP locality:
  - If destination EP is local then traffic is sent to the preferred Service-Chain, provided it is operational. At the end this must be considered intra-site traffic
  - If destination EP is remote, then traffic is forwarded by a permit rule towards the destination site. The first VTEP in the destination site (the BGW) will apply the redirect and send it to the preferred Service-Chain, provided it is operational

© 2025 Cisco and/or its affiliates. All rights reserved.

GPO Based Service Redirection

Centralized Service-Chain Deployment with Multi-Site

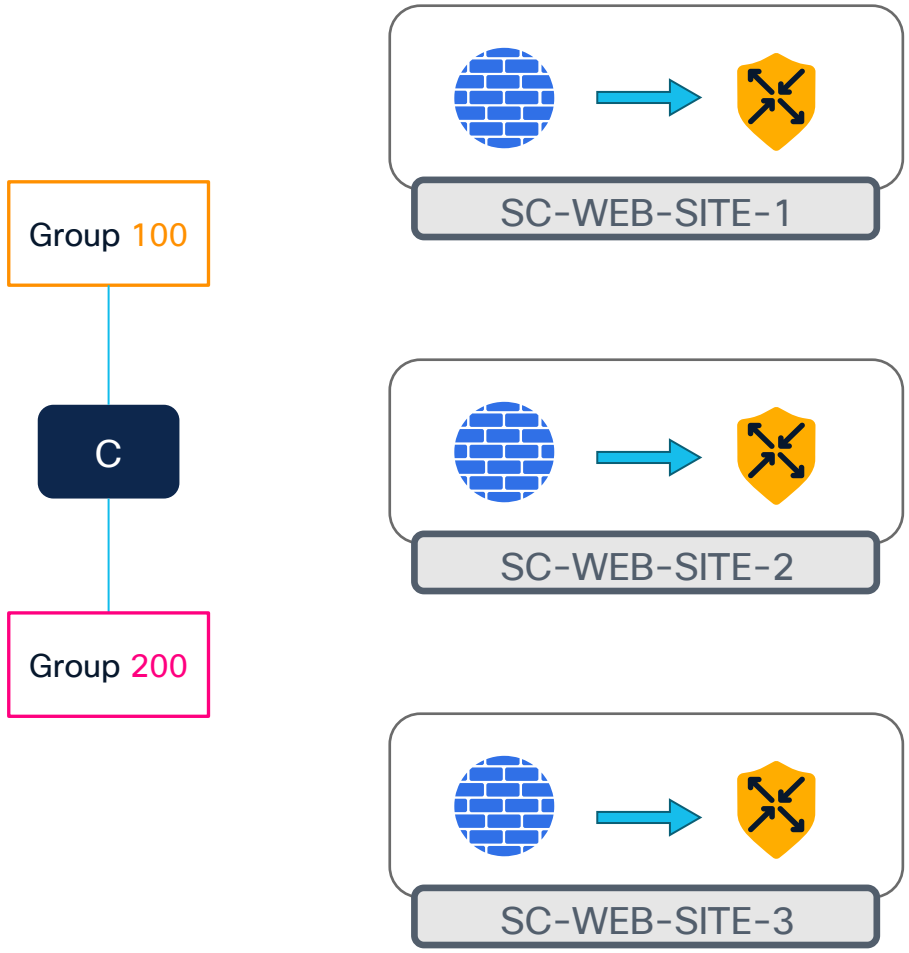
- A Service-Chain can be deployed only in a single fabric
  - Always consider the latency increase when redirecting flows to that centralized fabric



© 2025 Cisco and/or its affiliates. All rights reserved.

GPO Based Service Redirection

Multi-Site Service-Chain Redundancy

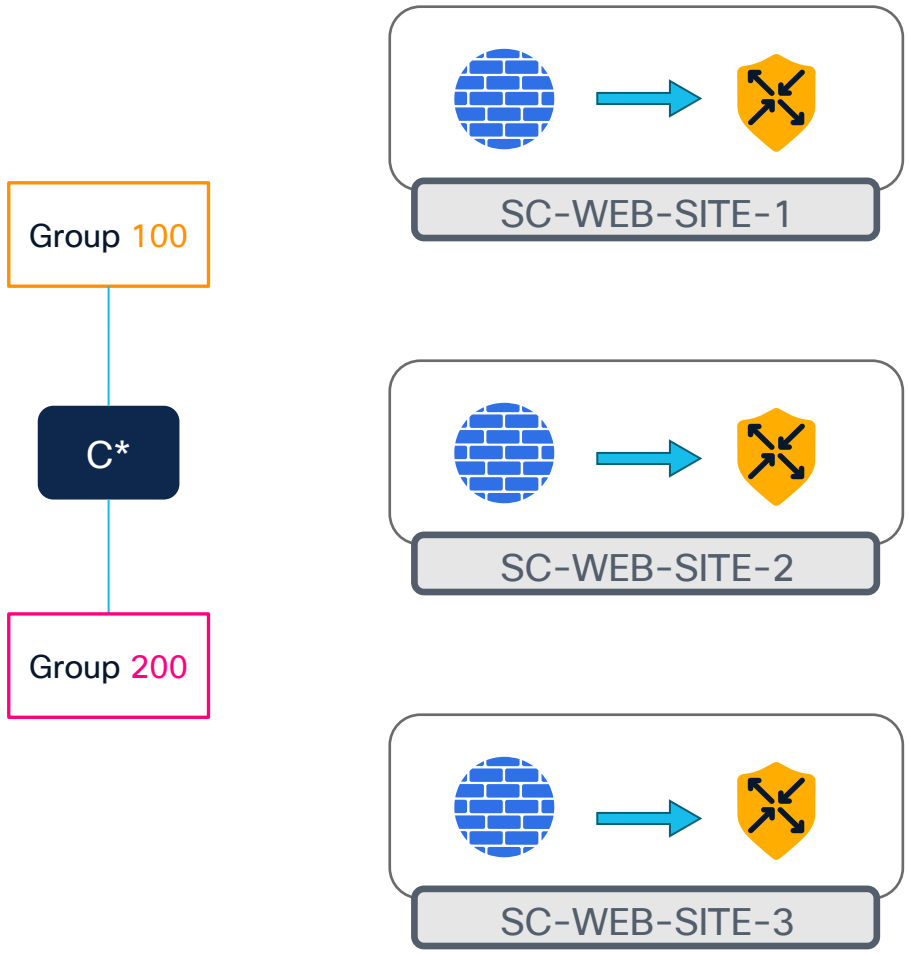


- Each redirection policy requires a favourite Service Chain
  - Can be deployed in the local fabric
  - Can be deployed remotely and reachable via the BGWs
- VTEPs in the same site must point to the same Service Chain
- Support configuration of backup Service Chains
  - When the primary Service Chain fails, the VTEPs will look at the Failover Group configuration containing the backup ones
  - Backups Service Chains are considered valid if they have the same number of functions. They must be configured everywhere
- Carefully design the redundancy, despite using a remote Service Chain as backup is technically possible, it might have a bad impact on the application

© 2025 Cisco and/or its affiliates. All rights reserved.

GPO Based Service Redirection

Multi-Site Service-Chain Redundancy



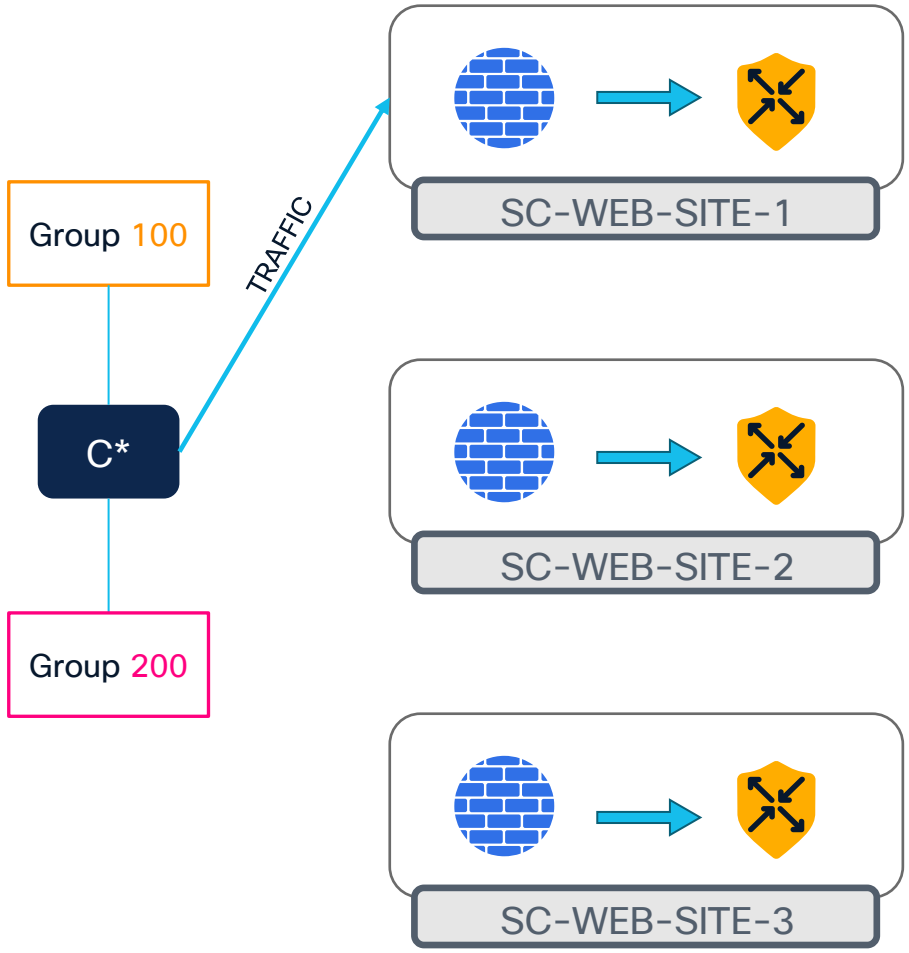
Configuration for Site-1 VTEPs

```
epbr service-chain SERVICE-CHAIN-WEB-SITE-1
  mode multisite failover-group SERVICE-CHAIN-WEB-FOVER
  10 set service FIREWALL-SITE-1 fail-action bypass
  20 set service IDS-SITE-1 fail-action drop

epbr service-chain SERVICE-CHAIN-WEB-SITE-2
  10 set service FIREWALL-SITE-2 fail-action bypass
  20 set service IDS-SITE-2 fail-action drop

epbr service-chain SERVICE-CHAIN-WEB-SITE-3
  ... [same but pointing to site 3 Service Functions ]

epbr failover-group SERVICE-CHAIN-WEB-FOVER
 service-chain SERVICE-CHAIN-WEB-SITE-2 preference 2
 service-chain SERVICE-CHAIN-WEB-SITE-3 preference 1
```

© 2025 Cisco and/or its affiliates. All rights reserved.

GPO Based Service Redirection

Multi-Site Service-Chain Redundancy



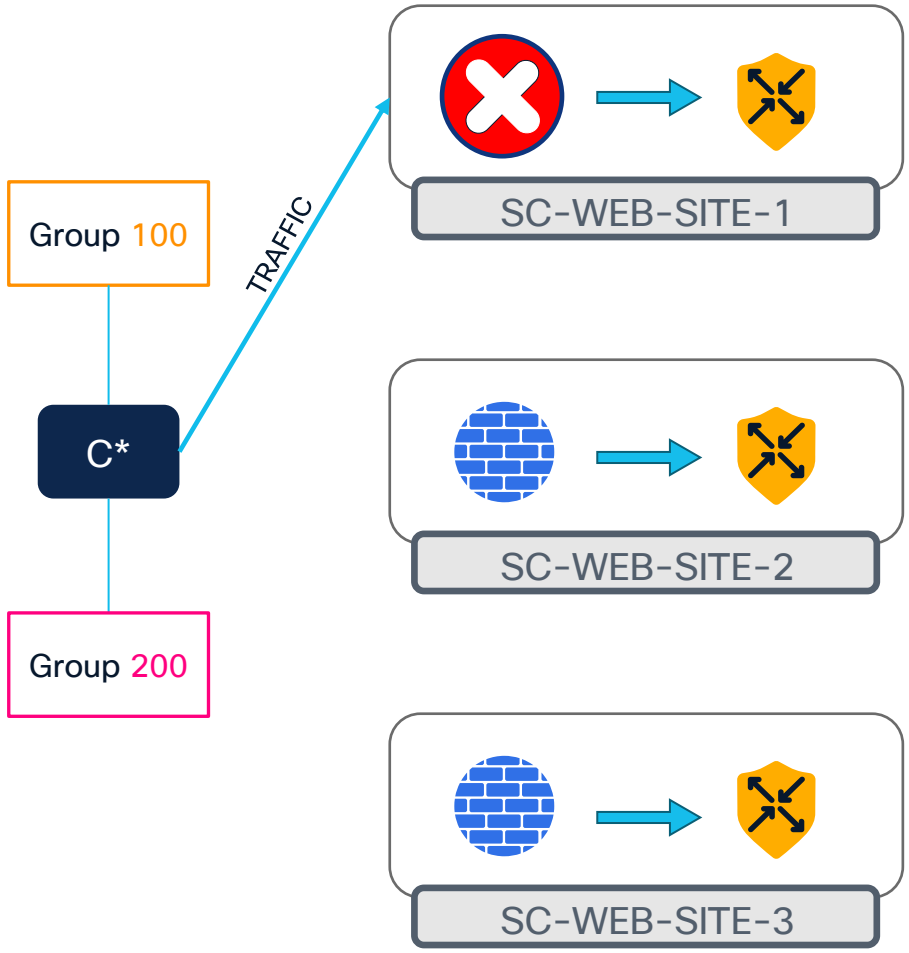
Configuration for Site-1 VTEPs

```
epbr service-chain SERVICE-CHAIN-WEB-SITE-1
  mode multisite failover-group SERVICE-CHAIN-WEB-FOVER
  10 set service FIREWALL-SITE-1 fail-action drop
  20 set service IDS-SITE-1 fail-action drop

epbr service-chain SERVICE-CHAIN-WEB-SITE-2
  10 set service FIREWALL-SITE-2 fail-action bypass
  20 set service IDS-SITE-2 fail-action drop

epbr service-chain SERVICE-CHAIN-WEB-SITE-3
  ... [same but pointing to site 3 Service Functions ]

epbr failover-group SERVICE-CHAIN-WEB-FOVER
 service-chain SERVICE-CHAIN-WEB-SITE-2 preference 2
 service-chain SERVICE-CHAIN-WEB-SITE-3 preference 1
```

© 2025 Cisco and/or its affiliates. All rights reserved.

GPO Based Service Redirection

Multi-Site Service-Chain Redundancy



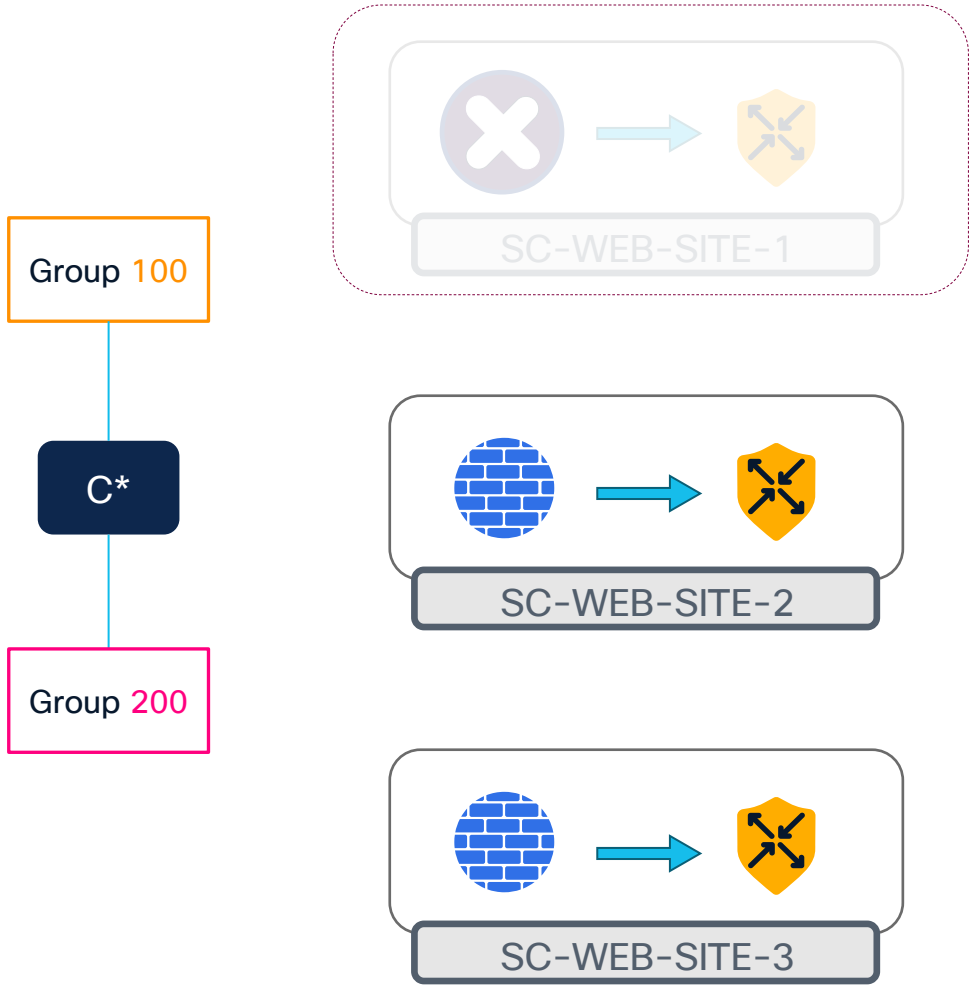
Configuration for Site-1 VTEPs

```
epbr service-chain SERVICE-CHAIN-WEB-SITE-1
  mode multisite failover-group SERVICE-CHAIN-WEB-FOVER
  10 set service FIREWALL-SITE-1 fail-action drop
  20 set service IDS-SITE-1 fail-action drop

epbr service-chain SERVICE-CHAIN-WEB-SITE-2
  10 set service FIREWALL-SITE-2 fail-action bypass
  20 set service IDS-SITE-2 fail-action drop

epbr service-chain SERVICE-CHAIN-WEB-SITE-3
  ... [same but pointing to site 3 Service Functions ]

epbr failover-group SERVICE-CHAIN-WEB-FOVER
 service-chain SERVICE-CHAIN-WEB-SITE-2 preference 2
 service-chain SERVICE-CHAIN-WEB-SITE-3 preference 1
```

© 2025 Cisco and/or its affiliates. All rights reserved.

GPO Based Service Redirection

Multi-Site Redundancy



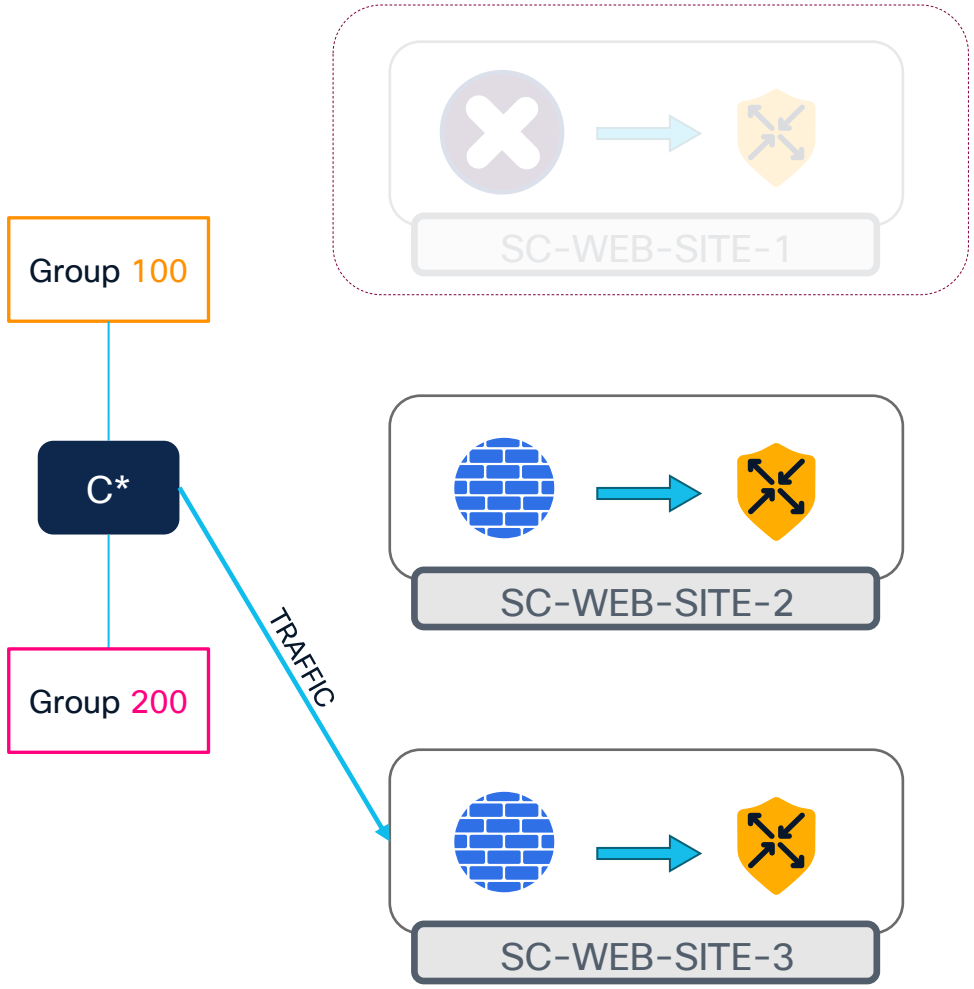
Configuration for Site-1 VTEPs

```
epbr service-chain SERVICE-CHAIN-WEB-SITE-1
  mode multisite failover-group SERVICE-CHAIN-WEB-FOVER
  10 set service FIREWALL-SITE-1 fail-action drop
  20 set service IDS-SITE-1 fail-action drop

epbr service-chain SERVICE-CHAIN-WEB-SITE-2
  10 set service FIREWALL-SITE-2 fail-action bypass
  20 set service IDS-SITE-2 fail-action drop

epbr service-chain SERVICE-CHAIN-WEB-SITE-3
  ... [same but pointing to site 3 Service Functions ]

epbr failover-group SERVICE-CHAIN-WEB-FOVER
 service-chain SERVICE-CHAIN-WEB-SITE-2 preference 2
service-chain SERVICE-CHAIN-WEB-SITE-3 preference 1
```

© 2025 Cisco and/or its affiliates. All rights reserved.

GPO Based Service Redirection

Multi-Site Redundancy



Configuration for Site-1 VTEPs

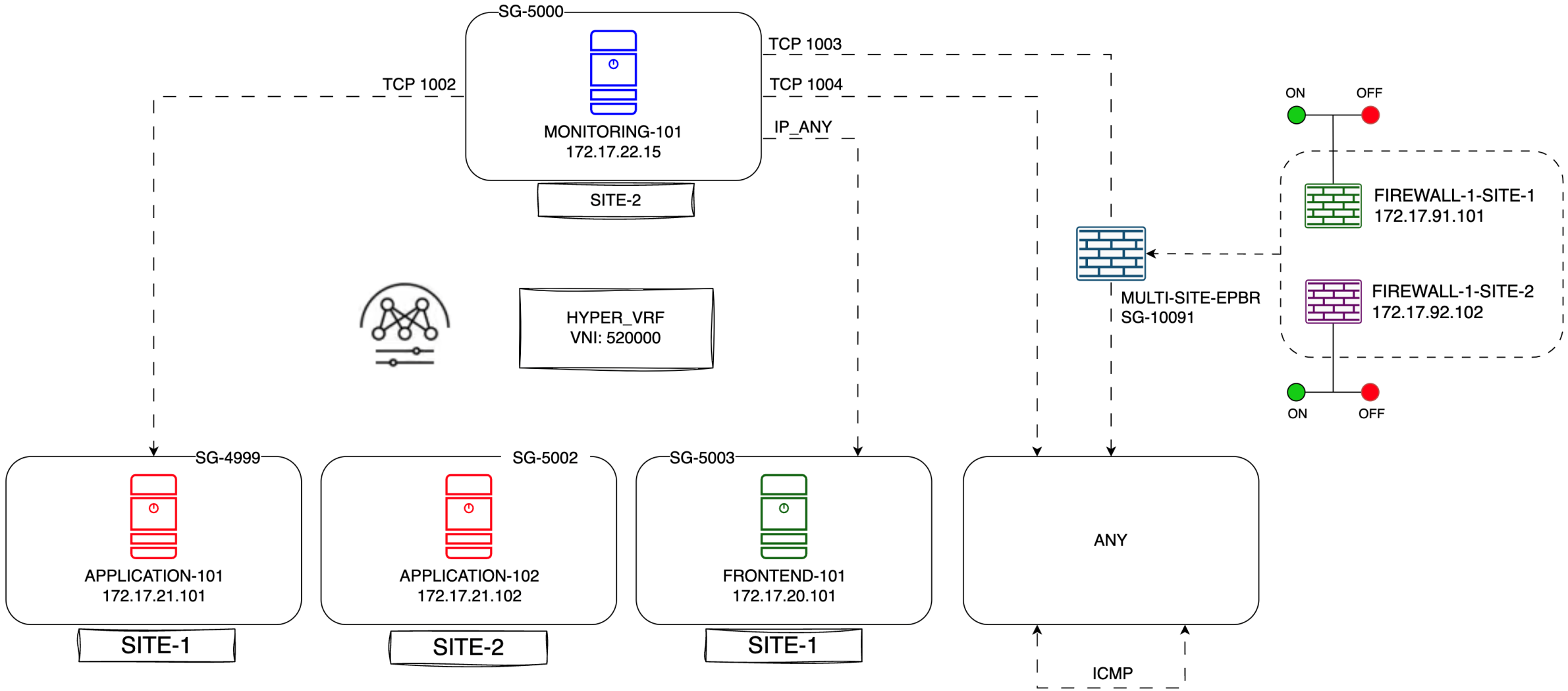
```
epbr service-chain SERVICE-CHAIN-WEB-SITE-1
  mode multisite failover-group SERVICE-CHAIN-WEB-FOVER
  10 set service FIREWALL-SITE-1 fail-action drop
  20 set service IDS-SITE-1 fail-action drop

epbr service-chain SERVICE-CHAIN-WEB-SITE-2
  10 set service FIREWALL-SITE-2 fail-action bypass
  20 set service IDS-SITE-2 fail-action drop

epbr service-chain SERVICE-CHAIN-WEB-SITE-3
  ... [same but pointing to site 3 Service Functions ]

epbr failover-group SERVICE-CHAIN-WEB-FOVER
 service-chain SERVICE-CHAIN-WEB-SITE-2 preference 2
 service-chain SERVICE-CHAIN-WEB-SITE-3 preference 1
```

© 2025 Cisco and/or its affiliates. All rights reserved.

Demo #2

Demo 2

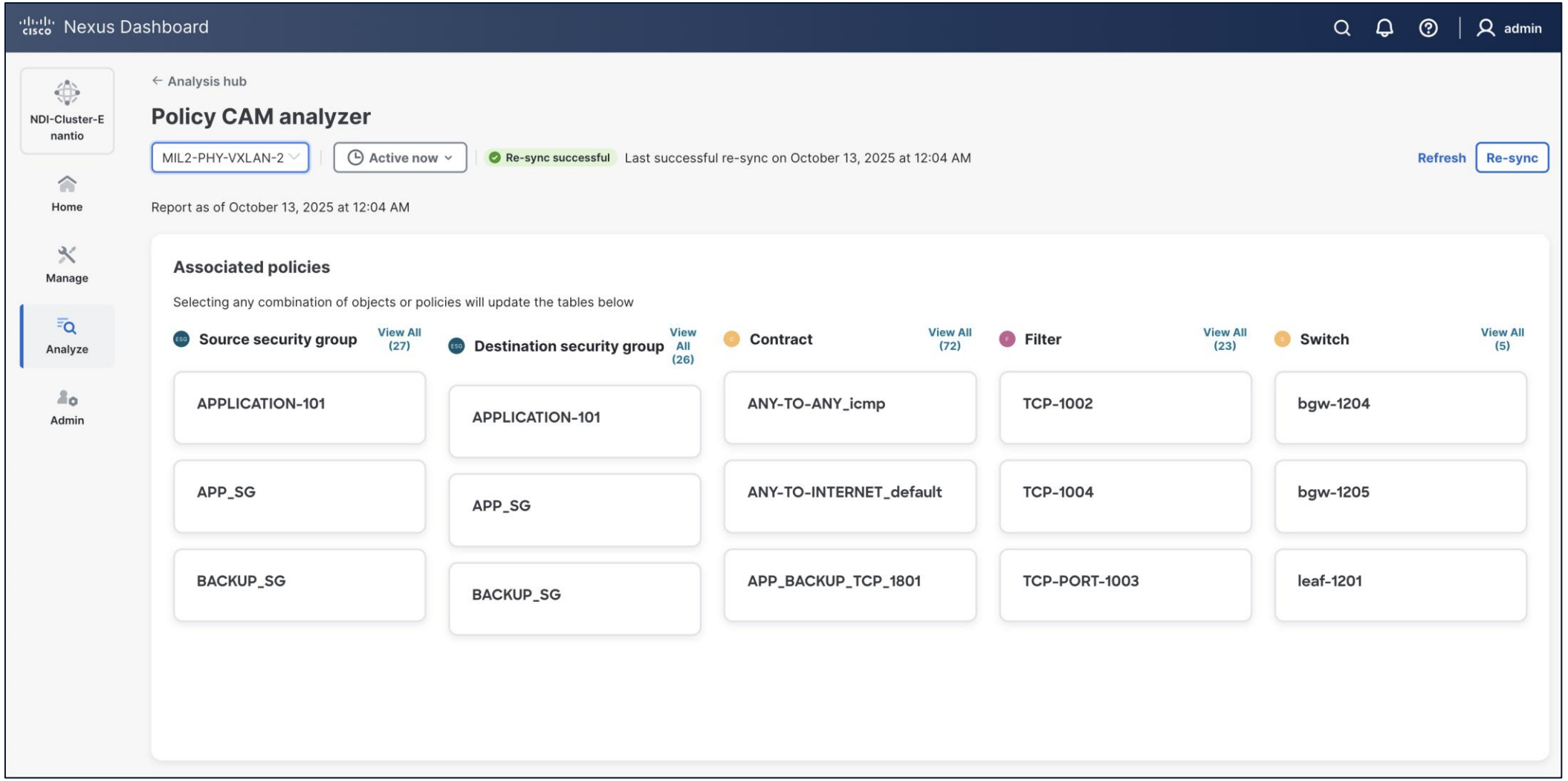
Topology



© 2025 Cisco and/or its affiliates. All rights reserved.

Verification

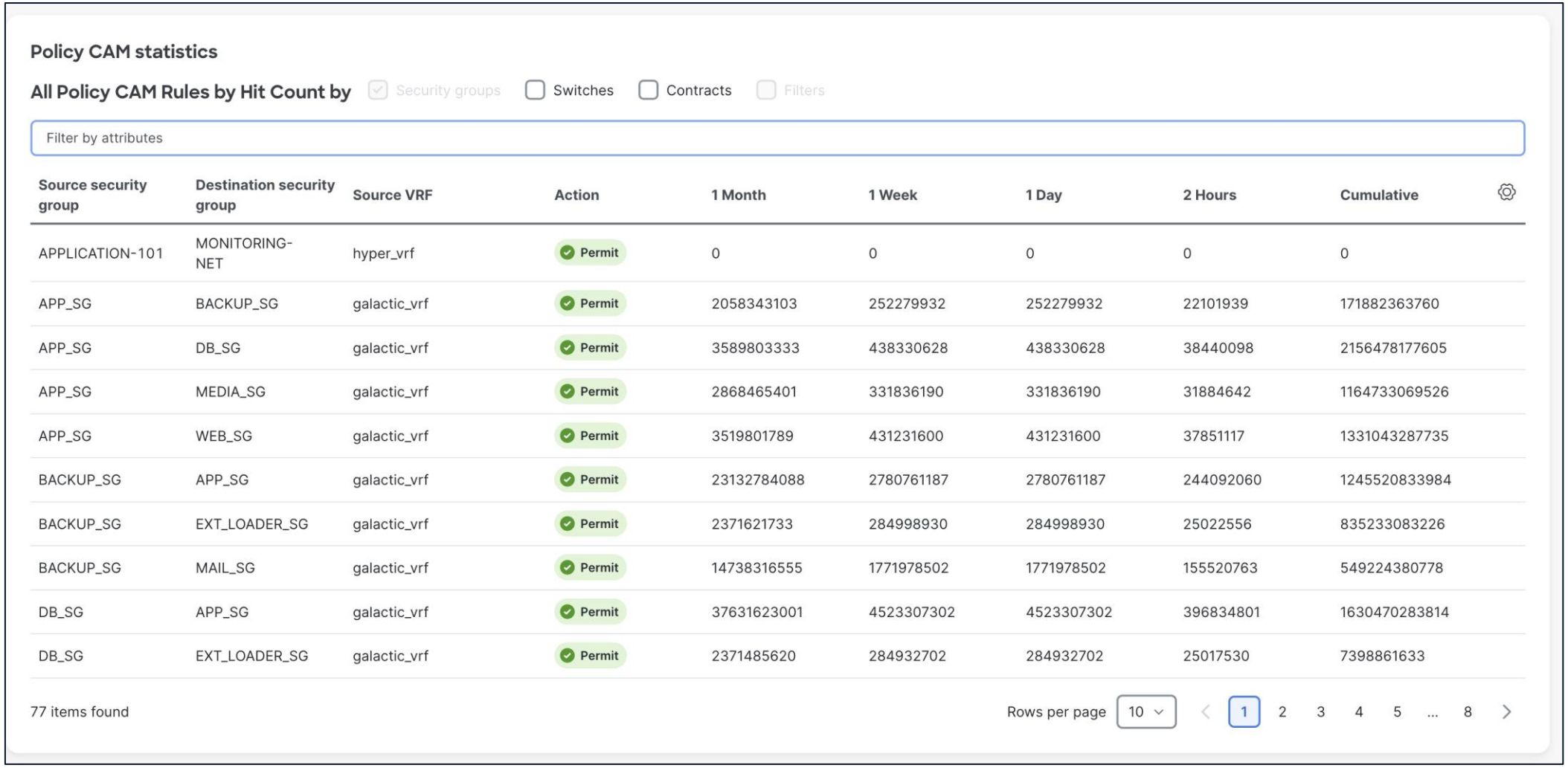
Policy CAM Analyzer



© 2025 Cisco and/or its affiliates. All rights reserved.

Verification

Policy CAM Statistics



Policy CAM statistics

All Policy CAM Rules by Hit Count by ☑ Security groups ☐ Switches ☐ Contracts ☐ Filters

Filter by attributes

Source security group	Destination security group	Source VRF	Action	1 Month	1 Week	1 Day	2 Hours	Cumulative
APPLICATION-101	MONITORING-NET	hyper_vrf	Permit	0	0	0	0	0
APP_SG	BACKUP_SG	galactic_vrf	Permit	2058343103	252279932	252279932	22101939	171882363760
APP_SG	DB_SG	galactic_vrf	Permit	3589803333	438330628	438330628	38440098	2156478177605
APP_SG	MEDIA_SG	galactic_vrf	Permit	2868465401	331836190	331836190	31884642	1164733069526
APP_SG	WEB_SG	galactic_vrf	Permit	3519801789	431231600	431231600	37851117	1331043287735
BACKUP_SG	APP_SG	galactic_vrf	Permit	23132784088	2780761187	2780761187	244092060	1245520833984
BACKUP_SG	EXT_LOADER_SG	galactic_vrf	Permit	2371621733	284998930	284998930	25022556	835233083226
BACKUP_SG	MAIL_SG	galactic_vrf	Permit	14738316555	1771978502	1771978502	155520763	549224380778
DB_SG	APP_SG	galactic_vrf	Permit	37631623001	4523307302	4523307302	396834801	1630470283814
DB_SG	EXT_LOADER_SG	galactic_vrf	Permit	2371485620	284932702	284932702	25017530	7398861633

77 items found

Rows per page 10 < 1 2 3 4 5 ... 8 >

© 2025 Cisco and/or its affiliates. All rights reserved.

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 NDFC*
  - Automation can be achieved in both environments
  - Automation can integrate external data sources and/or logics

*GPO Service Redirection workflows: future NDFC

© 2025 Cisco and/or its affiliates. All rights reserved.

Complete your session evaluations

Complete a minimum of 4 session surveys and the Overall Event Survey to claim a Cisco Live T-Shirt.

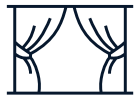
Earn up to 800 points by completing all surveys and climb the Cisco Live Challenge leaderboard.

Level up and earn exclusive prizes!

Complete your surveys in the Cisco Live Events app.

© 2025 Cisco and/or its affiliates. All rights reserved.

Continue your education



Visit the Cisco Stand for related demos

Book your one-on-one Meet the Expert meeting

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

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

© 2025 Cisco and/or its affiliates. All rights reserved.

Thank you

© 2025 Cisco and/or its affiliates. All rights reserved.

CISCO