Hewlett Packard Enterprise

HPE aruba networking

AOS-CX 10.13 Update: Reserved GBP Tag for Internet Traffic

Corey Dow, Technical Marketing Engineer

November 28th , 2023

Agenda

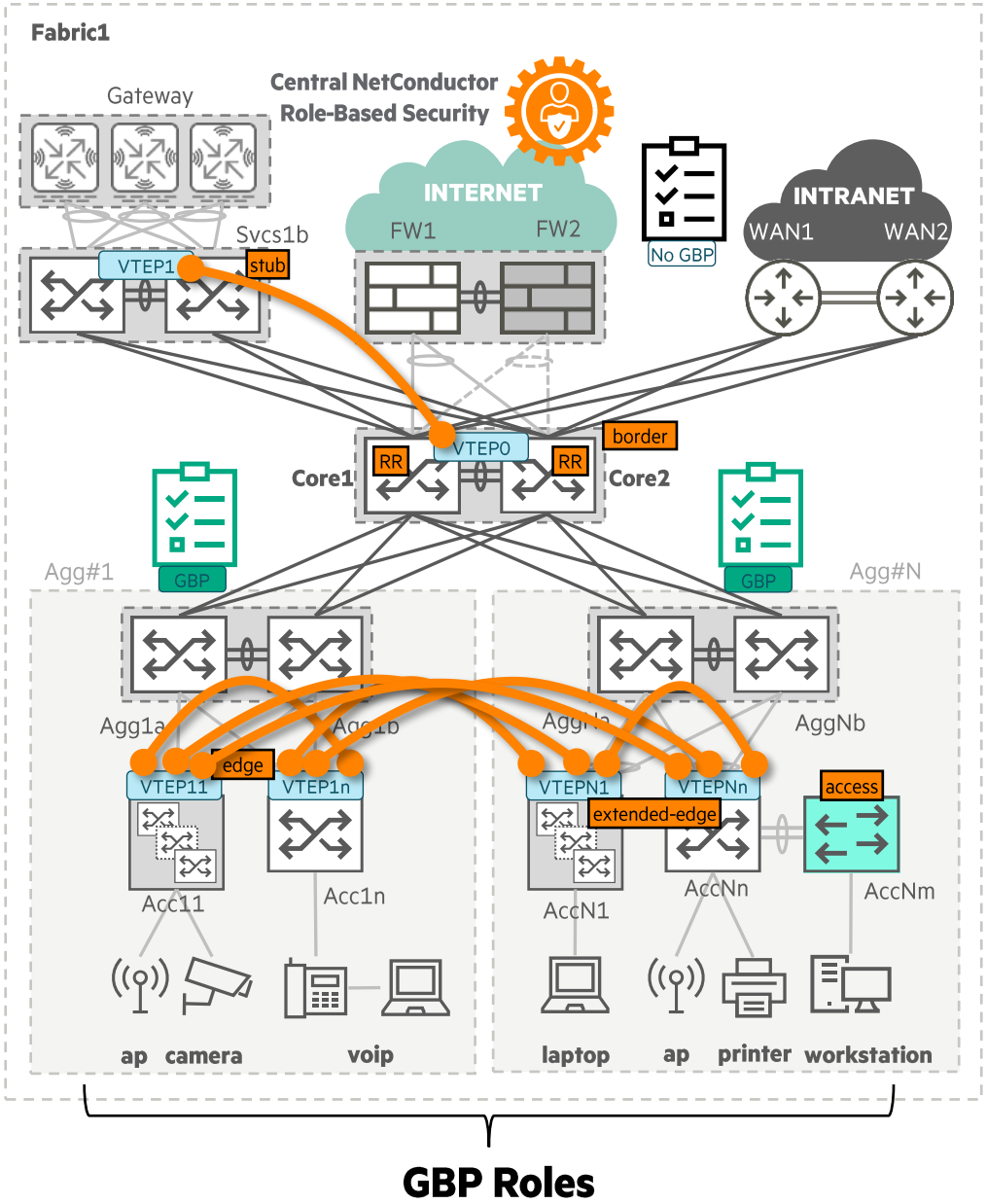
1	Overview
2	Use Cases
3	Details
4	Configuration
5	Best Practices
6	Troubleshooting
7	Demo

Overview

GBP (Group Based Policy) Overview

Introduction

- Also known as **Virtual Network Based Tunneling** (VNBT) or **Group Policy Option** (GPO)
- Establishes a mechanism for Role Based Access Control within an **EVPN-VXLAN** fabric
  - Policy ids are mapped to user or device roles
  - Egress VTEPs have configured group-based policies that determine whether the source role is authorized to communicate with the destination role
    - Intra Role communication is permitted by default
    - Inter Role communication is denied by default
- **Local User Roles** are assigned to each of the authenticated devices that have associated Group Based Policies
- **Macro or Micro-segmentation** scenarios supported
  - Inter-VNI or Intra-VNI
- **Aruba Central NetConductor** orchestrates and automates the provisioning of roles and policy creation



GBP (Group Based Policy) Overview

Resources for prior releases

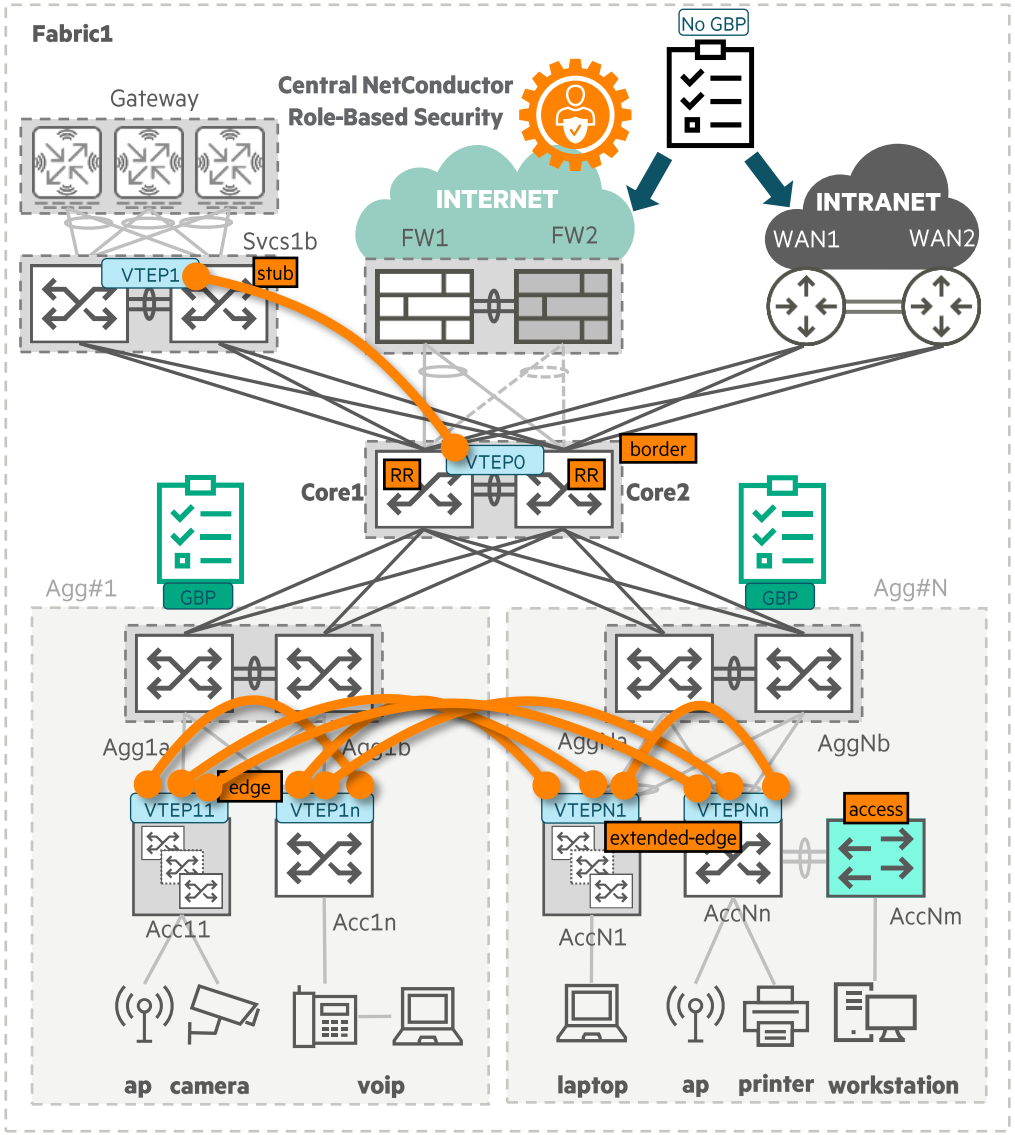
- Feature first introduced in AOS-CX 10.08 for single fabric and Stub VTEPs
- Extended to Multi-Fabric EVPN-VXLAN support in AOS-CX Release 10.11
- Orchestration of fabrics and roles added with ACN 2.5.7

Aruba Central NetConductor & Aruba CX Better Together

Aruba AOS-CX 10.11 Update - Multi-Fabric VXLAN GBP

Aruba AOS-CX 10.08 Update - VNBT-VXLAN GBP

Aruba AOS-CX 10.08 Update - VXLAN Stub VTEP

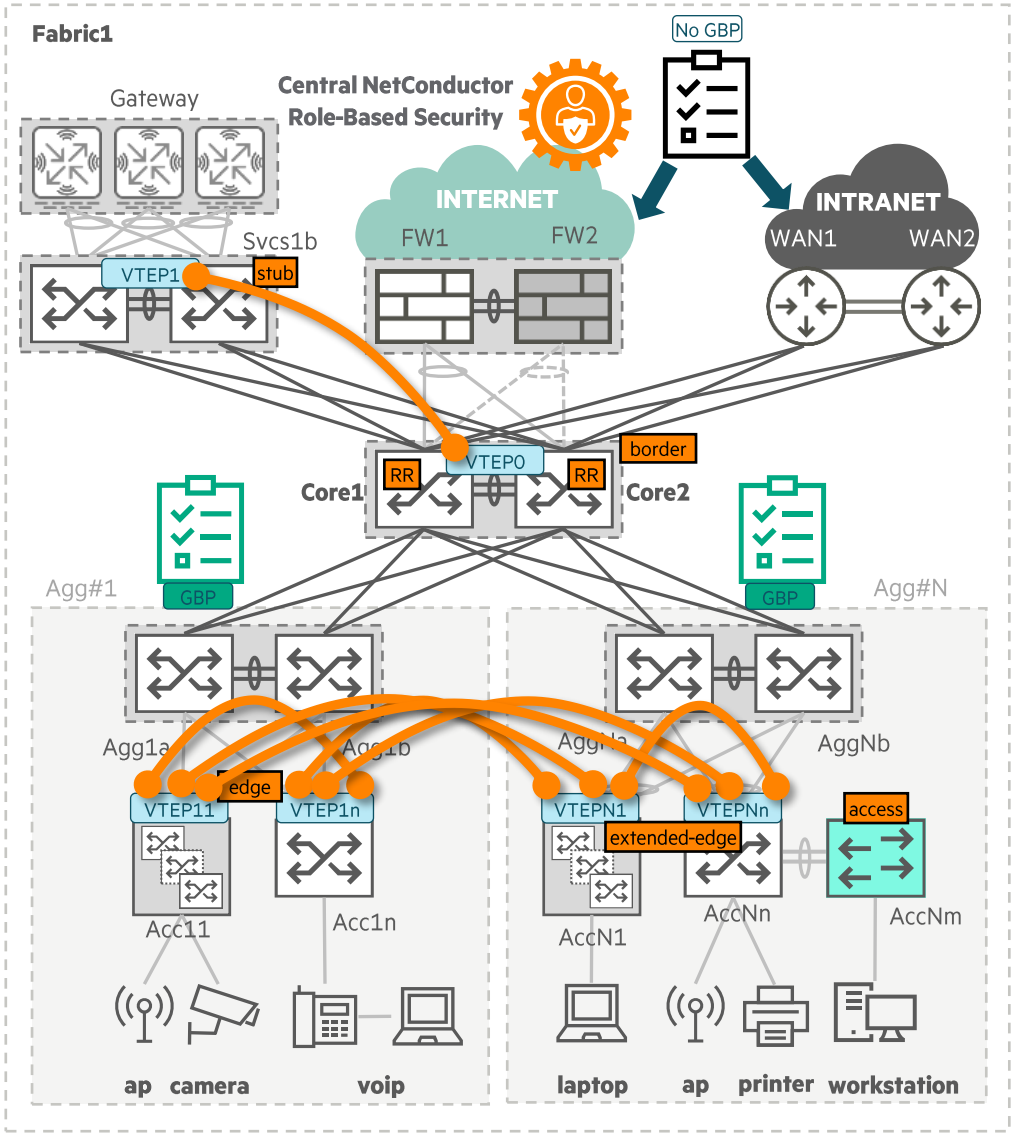


Reserved GBP Tag for Internet/Intranet Traffic

What is New with AOS-CX Release 10.13?

- Missing was the ability to **tag traffic**, at the border VTEP, arriving from external networks, i.e., Intranet/Internet
- GBP is applied at the ingress VTEP post-authentication with **MAC/802.1X authentication**, but traffic arriving from External networks are not initially tagged with **any Group Policy Ids**
- To support policy enforcement with **North-South and South-North** traffic flows, in addition to East-West, we needed to provide this capability
- Reserved Group Based Policy ID Tags were added to AOS-CX 10.13 for **Internet (3)**, **Intranet (4)**, and the **ISL (5)**
- An 8360v1/v2 core/border VTEP may now apply policies to map **non-GBP tagged traffic** with **GBP reserved roles** for Internet or Intranet
- Policy enforcement occurs at the **Egress VTEPs** and now **Border VTEPs with Role Based Access Lists and AOS-CX 10.13**

```
> Ethernet II, Src: ArubaaHe_a5:9f:40 (b8:d4:e7:a5:9f:40), Dst: ArubaaHe_b7:b5:00 (64:e8:81:b7:b5:00)
> Internet Protocol Version 4, Src: 192.168.0.3, Dst: 192.168.0.1
> User Datagram Protocol, Src Port: 54284, Dst Port: 4789
v Virtual eXtensible Local Area Network
  v Flags: 0x8800, GBP Extension, VXLAN Network ID (VNI)
      1... .... .... .... = GBP Extension: Defined
      .... .... .0.. .... = Don't Learn: False
      .... 1... .... .... = VXLAN Network ID (VNI): True
      .... .... .... 0... = Policy Applied: False
      .000 .000 0.00 .000 = Reserved(R): 0x0000
    Group Policy ID: 300
    VXLAN Network Identifier (VNI): 200
    Reserved: 0
> Ethernet II, Src: ArubaaHe_a5:9f:40 (b8:d4:e7:a5:9f:40), Dst: aa:aa:aa:00:00:02 (aa:aa:aa:00:00:02)
> Internet Protocol Version 4, Src: 192.168.201.200, Dst: 192.168.200.100
> Data (986 bytes)
```



GBP Feature Platform Support

Feature Review and Updates

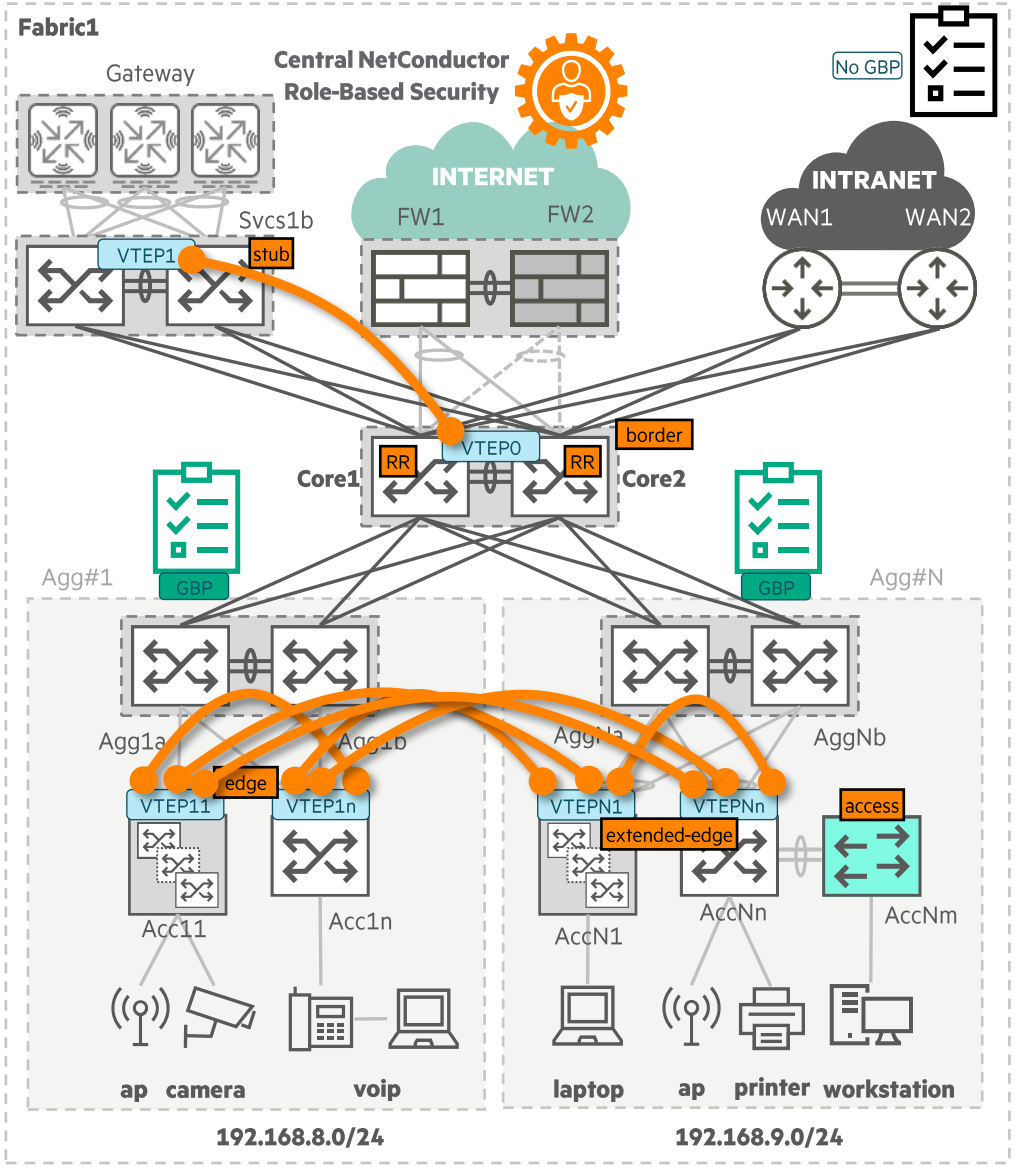
- Border VTEP GBP Tag relay
  - 8325/10K added with 10.12.0006
- GBP Reserved Internet/Intranet/ISL Roles
  - 6200, 6300, 6400, 8100 and 8360v1/v2
- GBP Role Access List / Intranet role mapping
  - **8360v1/v2 Only**
  - Requires **Core-Spine** profile

	Feature	4100i 6000 6100	6200	6300	6400	8100	8320	8325	8360	8400	9300	10000	OVA
	GBP Policy Enforcement	No	Yes	Yes	Yes	Yes	No	No	Yes	No	No	No	No
10.12.0006	Border VTEP GBP Tag Relay	No	No	Yes	Yes	No	No	Yes	Yes	No	No	Yes	No
10.13.0005	GBP Reserved Internet/Intranet/ISL Roles	No	Yes	Yes	Yes	Yes	No	No	Yes	No	No	No	No
10.13.0005	GBP ACL role-access-list	No	No	No	No	No	No	No	Yes	No	No	No	No
10.13.0005	GBP Intranet role mapping with object group lists	No	No	No	No	No	No	No	Yes	No	No	No	No

Use Cases

Use Cases
Reserved GBP Tags

- Internet traffic can ingress/egress the border VTEP with different encapsulations, e.g., VXLAN third-party, MPLS, that may or may not have GBP policy associations
- Intranet traffic to/from other fabrics can also exit/enter the border VTEP
- There is nothing like internet VRF on the border VTEPs
  - In most of our deployments, the internet RIB is hosted on the WAN-Edge Box and the Internet VRFs have a footprint only on the WAN-E not on the border VTEP
  - Enterprise VRFs are extended up to the WAN-E, therefore both internet and inter-fabric traffic enter/exit the border on the Enterprise VRFs
- We solve that problem, on the border VTEPs, by associating GBP roles, i.e., Intranet or Internet with subnets where we want segmentation
- Partial Internet Traffic Suppression
  - There can be cases where traffic to/from some websites are to be allowed and the rest of the internet traffic needs to be denied
    - From Guest traffic to www.hpe.com and www.arubanetworks.com are allowed but all other traffic is denied
- Forwarding over VSX ISL
  - Border VSX connected to WAN Edge with link loss
    - Traffic redirected through the border VTEPs ISL link



Details

Details

- **GPB-MAC, GBP-IPv4** and **GBP-IPv6** based classes
  - Cannot be configured under classifier or port access policies as match criteria
  - All destination roles in class entry match conditions **must** be of the same role
    - For example, the iot class below needs to have all the same destination roles, i.e., “iot” not “guest”

```
class gbp-ip class_iot
    10 match icmp internet iot
    20 match icmp intranet iot
    30 match tcp intranet eq ssh guest
```

- Single or Multi-Fabric EVPN-VXLAN deployments
- The Group-based port-access policies support the following actions:
  - drop : drop the packet
  - 6300, 6400 **(New with 10.13)**
    - Reflect : enable the switch to allow the packet only if the flow is initiated by the client (Covered in the Reflexive Policy TOI session)
- Group-based port-access policies are associated and applied via **local user roles (LUR)**
  - Downloadable User Roles (DUR) are not supported
- New **reserved** system roles **- internet(3)**, **intranet(4)**, and **isl(5)** are introduced **(New with 10.13)**
  - May be remapped if **policy IDs** 3, 4 and 5 are currently used
- GBP Intranet role to object group mapping **(New with 10.13)**
  - Commands applicable to **profile core-spine** only **(8360v1/v2)**
  - Object groups contain lists of IPv4/IPv6 prefixes that will have the **Intranet role** applied
  - A **unique** object group is required **per VRF**
- GBP Role ACLs are introduced **(New with 10.13)**
  - Commands applicable to **profile core-spine** only **(8360v1/v2)**
  - Applied at the border VTEPs to perform traffic filtering with role-based policies to **north-south traffic** arriving from **Intranet/Internet** sources
    - For example, only allow designated traffic with the **Intranet role** to destination **role camera**

Configuration

Configuration

Overview of steps to create a GBP Policy for Internet/Intranet Roles

- **WAN Edge Border VTEPs**
  - Switch the **8360v1/v2 profile** from **aggregation-leaf(default)** to **core-spine** and reboot
  - Create IPv4 and IPv6 Object Groups with match prefixes for **Intranet Subnets**
    - Prefixes **not** included will **inherit** the **Internet role**
    - Map GBP role intranet to those configured Object Groups
  - Create GBP IPv4/IPv6 ACLs permitting or denying access
  - Apply the configured ACLs as a global policy
    - Not tied to specific interfaces or VLANs by nature of it being a Role Based ACL
  - Enable GBP
- **Egress Edge/Access VTEPs**
  - Configure **GBP** MAC, IPv4/IPv6 classes with match actions for the source and destination roles and protocols
    - New source roles for internet, intranet and isl are reserved starting with 10.13
    - All the entries in a GBP class need to have the same destination role name
    - These classes **cannot** be configured under classifier or port access policies as match criteria
  - Create Port-Access **GBP** policies that include those classes
  - Associate Port-Access roles with created GBP policies
  - Enable GBP

Configuration

Confirm Role to Group Policy ID Mapping

- New reserved roles are available for mapping internet, intranet and ISL roles on border VTEPs

```
gbp enable
gbp role camera 110
gbp role infra 2
gbp role internet 3
gbp role intranet 4
gbp role isl 5
gbp role printer 100
gbp role signage 120
```

8360v1/v2

- New reserved roles are available for mapping internet and intranet roles on Access EDGE VTEPs

```
gbp enable
gbp role camera 110
gbp role infra 2
gbp role internet 3
gbp role intranet 4
gbp role printer 100
gbp role signage 120
```

6200
6300
6400
8100

Configuration

WAN Edge Border VTEPs

- Switch the **8360v1/v2 profile** from **aggregation-leaf** to **core-spine** and reboot

```
8360-01(config)# profile core-spine
Save this config and reboot the switch for the
changes to take effect
```

- Create IPv4 and IPv6 Object Groups with match prefixes for Intranet Subnets

```
object-group ip address v4prefixes
vrf vrf1
10 11.1.0.0/255.255.0.0
20 12.1.0.0/255.255.0.0
30 13.1.0.0/255.255.0.0
! Intranet IPv4 prefixes

object-group ipv6 address v6prefixes
vrf vrf1
10 11:1:1::/64
20 12:1:1::/64
30 13:1:1::/64
! Intranet IPv6 prefixes
```

- Associate the **object groups** with the **"Intranet"** role

```
8360-01(config)# gbp role intranet object-group ip v4prefixes
8360-01(config)# gbp role intranet object-group ipv6 v6prefixes
```

- Create **GBP IPv4/IPv6 ACLs** permitting or denying access
  - Permits any IPv4 traffic from role **iot** to 69.1.1.0/24
  - Permits any IPv6 traffic from role **iot** to 69:1:1::0/64

```
gbp role-access-list ip inet-acl
     10 permit iot 69.1.1.0/255.255.255.0 vrf vrf1
gbp role-access-list ipv6 v6inet-acl
     10 permit iot 69:1:1::0/64 vrf vrf1
```

- Apply the configured ACLs as a global policy

```
8360-01(config)# apply gbp role-access-list ip inet-acl
8360-01(config)# apply gbp role-access-list ipv6 v6inet-acl
```

- Enable GBP

```
8360-01(config)# gbp enable
```

Configuration

Egress Edge/Access VTEPs – 6200/6300/6400/8100/8360 Platforms

- Configure **GBP** MAC, IPv4/IPv6 classes with match actions for the source and destination roles and protocols

GBP IPv4

```
class gbp-ip class_iot
    10 match icmp internet iot
    20 match udp internet eq snmp iot
    30 match icmp intranet iot
    40 match tcp intranet eq ssh iot
    50 match udp intranet eq snmp iot
    60 match tcp intranet eq rdp iot
```

GBP IPv6

```
class gbp-ipv6 class_iot
    10 match icmpv6 internet iot
    20 match udp internet eq snmp iot
    30 match icmpv6 intranet iot
    40 match tcp intranet eq ssh iot
    50 match udp intranet eq snmp iot
    60 match tcp intranet eq rdp iot
```

GBP MAC

```
class gbp-mac class_iot
    10 match any iot arp count
```

- Create Port-Access **GBP** policies that include those created GBP classes

```
port-access gbp policy_iot
    10 class gbp-ip class_iot
    20 class gbp-ipv6 class_iot
    30 class gbp-mac class_iot
```

- Associate Port-Access roles with created GBP policies

```
port-access role iot
    associate gbp policy_iot
    vlan access 10
```

- Enable GBP

```
switch(config)# gbp enable
```

REST Interfaces

GBP Role-Access-Lists

```
#!/bin/bash

curl --noproxy 127.0.0.1 -k -X POST \
-c /tmp/cookie \
-H 'Content-Type: multipart/form-data' \
"https://127.0.0.1/rest/v10.13/login" -F 'username=admin' -
F 'password=somepass'
```

Retrieve cookie to begin session

```
#!/bin/bash

curl -k --noproxy 127.0.0.1 -X POST -b /tmp/cookie \
"https://127.0.0.1/rest/v10.13/system/gbp_internet_role_acl
s" -H "accept: */*" \
-H "Content-Type: application/json" -d '{
"cfg_version":0,
"name": "myinet-acl",
"list_type":"ipv4"
}'
```

Create IPv4 Role Based Access List

```
#!/bin/bash

curl -k --noproxy 127.0.0.1 -X POST -b /tmp/cookie \
"https://127.0.0.1/rest/v10.13/system/gbp_internet_role_acl
s/myinet-acl,ipv4/cfg_aces" -H "accept: */*" \
-H "Content-Type: application/json" -d '{
"action": "permit",
"count": true,
"dst_ip": "192.168.0.56/255.255.255.255",
"sequence_number": 10,
"src_role": "iot",
"vrf": "/rest/v10.13/system/vrfs/VRF1"
}'
```

Add **"permit"** of source **role "iot"** to destination **"192.168.0.56"**

```
#!/bin/bash

curl -k --noproxy 127.0.0.1 -X PUT -b /tmp/cookie \
--url "https://127.0.0.1/rest/v10.13/system/gbp_internet_role_acls/myinet-
acl,ipv4" -d \
'{"cfg_version":1}'
```

Update the config version to apply the change to hardware

```
8360(config)# show gbp role-access-list commands
gbp role access-list ip myinet-acl
    10 permit iot 192.168.0.56 vrf VRF1 count
```

REST Interfaces

GBP Role-Access-Lists

GBP_INTERNET_ROLE_ACL

GET	/system/gbp_internet_role_acls
POST	/system/gbp_internet_role_acls
GET	/system/gbp_internet_role_acls/{GBP_INTERNET_ROLE_ACL.name},{GBP_INTERNET_ROLE_ACL.list_type}
PUT	/system/gbp_internet_role_acls/{GBP_INTERNET_ROLE_ACL.name},{GBP_INTERNET_ROLE_ACL.list_type}
PATCH	/system/gbp_internet_role_acls/{GBP_INTERNET_ROLE_ACL.name},{GBP_INTERNET_ROLE_ACL.list_type}
DELETE	/system/gbp_internet_role_acls/{GBP_INTERNET_ROLE_ACL.name},{GBP_INTERNET_ROLE_ACL.list_type}

GBP_INTERNET_ROLE_ACL_Entry

GET	/system/gbp_internet_role_acls/{GBP_INTERNET_ROLE_ACL.name},{GBP_INTERNET_ROLE_ACL.list_type}/cfg_aces
POST	/system/gbp_internet_role_acls/{GBP_INTERNET_ROLE_ACL.name},{GBP_INTERNET_ROLE_ACL.list_type}/cfg_aces
GET	/system/gbp_internet_role_acls/{GBP_INTERNET_ROLE_ACL.name},{GBP_INTERNET_ROLE_ACL.list_type}/cfg_aces /{GBP_INTERNET_ROLE_ACL_Entry.sequence_number}
PUT	/system/gbp_internet_role_acls/{GBP_INTERNET_ROLE_ACL.name},{GBP_INTERNET_ROLE_ACL.list_type}/cfg_aces /{GBP_INTERNET_ROLE_ACL_Entry.sequence_number}
PATCH	/system/gbp_internet_role_acls/{GBP_INTERNET_ROLE_ACL.name},{GBP_INTERNET_ROLE_ACL.list_type}/cfg_aces /{GBP_INTERNET_ROLE_ACL_Entry.sequence_number}
DELETE	/system/gbp_internet_role_acls/{GBP_INTERNET_ROLE_ACL.name},{GBP_INTERNET_ROLE_ACL.list_type}/cfg_aces /{GBP_INTERNET_ROLE_ACL_Entry.sequence_number}

Equivalent Configurations

AOS-CX configuration Comparisons

AOS-CX

```
gbp enable
gbp role camera 110
gbp role infra 2
gbp role internet 3
gbp role intranet 4
gbp role printer 100
gbp role signage 120

object-group ip address v4prefixes
vrf vrf1
10 11.1.0.0/255.255.0.0
20 12.1.0.0/255.255.0.0
30 13.1.0.0/255.255.0.0

object-group ipv6 address v6prefixes
vrf vrf1
10 11:1:1::/64
20 12:1:1::/64
30 13:1:1::/64

8360-01(config)# gbp role intranet object-group ip v4prefixes
8360-01(config)# gbp role intranet object-group ipv6 v6prefixes
```

Cisco-IOS XE

Cisco DNA Center

Cisco Calls it SGT ID

- **(Security Group Tag) – prior to SD-Access**
- **(Scalable Group Tag) - SD-Access**

```
cts role-based sgt-map 192.168.0.0/16 sgt 192
cts role-based sgt-map 192:168::/64 sgt 192
cts role-based sgt-map vrf green 10.2.201.10 sgt 101
cts role-based sgt-map vlan-list 101 sgt 101
cts role-based sgt-map vlan-list 102 sgt 102
```

SG ACLs = contracts
Policy Extended Nodes (PENS) = VTEP

EGRESS PEN provides the enforcement

VN = VNI

Security Group Firewalls (SGFWs) support policies that may be based on SGTs for networks outside the fabric

- Note: Cisco DNA has Security Group Firewalls (SGFWs) that are GPO/SGT tag aware
  - Those devices attach to the WAN Edge, so border manipulation of roles isn't needed as it is with AOS-CX

Equivalent Configuration

AOS-CX configuration comparisons

AOS-CX

```
gbp enable
gbp role camera 110
gbp role infra 2
gbp role internet 3
gbp role intranet 4
gbp role printer 100
gbp role signage 120

object-group ip address v4prefixes
vrf vrf1
10 11.1.0.0/255.255.0.0
20 12.1.0.0/255.255.0.0
30 13.1.0.0/255.255.0.0

object-group ipv6 address v6prefixes
vrf vrf1
10 11:1:1::/64
20 12:1:1::/64
30 13:1:1::/64

8360-01(config)# gbp role intranet object-
group ip v4prefixes
8360-01(config)# gbp role intranet object-
group ipv6 v6prefixes
```

H3C/HPE comware

NO GPO/GBP policies

AOS-S

NO GPO/GBP policies

Best Practices

Best Practices

- Configure all fabric subnets on the border into object groups that are assigned the Intranet role, otherwise they will inherit the Internet role
- Advise against sequencing policies or classes with 1,2,3,4,5 ; makes troubleshooting more challenging as you can't insert a rule without first resequencing them
- Be careful when defining 'any' role wildcards in policies
  - The following class provides inter-role communication, from any source role, which was not what the customer intended
  - 'arp' should have been used instead of 'any' protocol and it is better to define which source roles are permitted, instead of specifying 'any' source role

```
class gbp-mac iot_camera_ALLOW
    1 match any iot_camera any
```

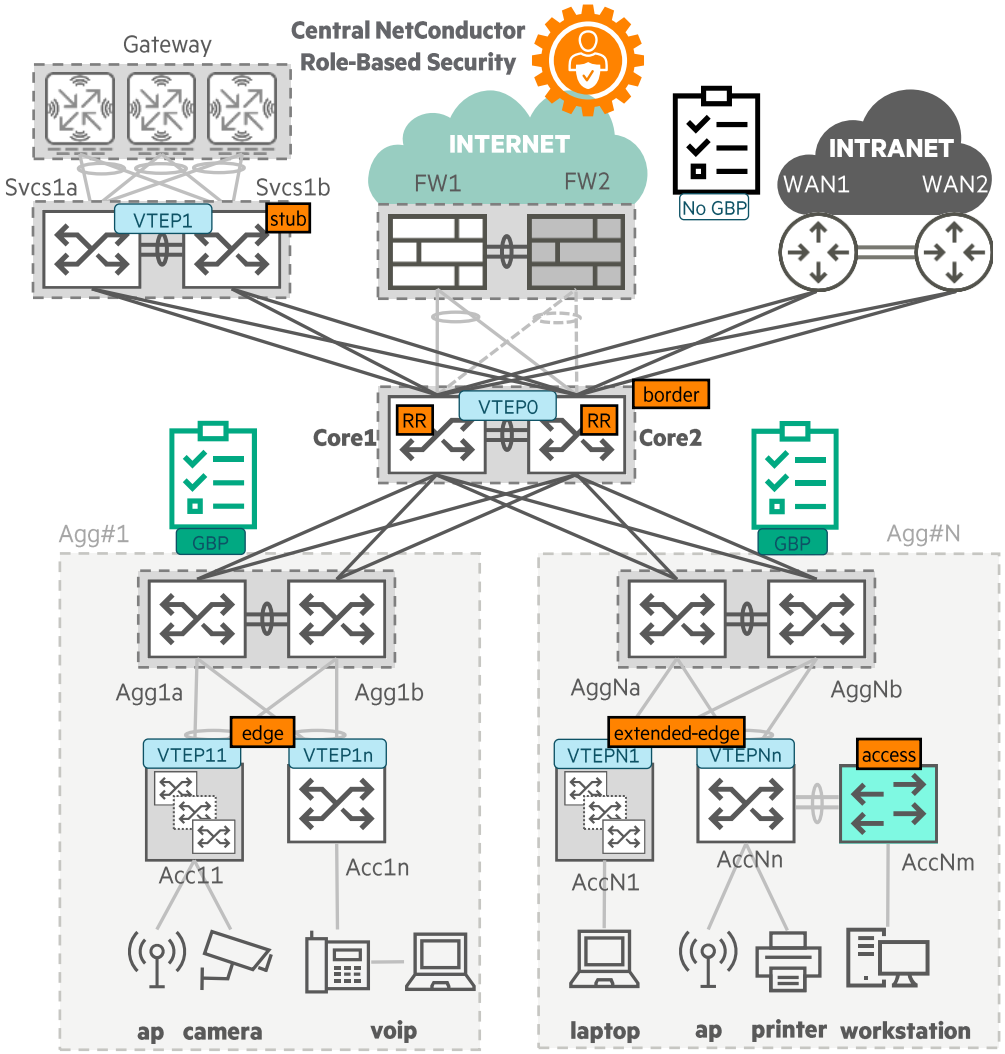
- Note that Role ACLs configured on the borders have an **implicit 'deny' rule for Internet** and default role but an **implicit 'permit' rule** for prefixes in object groups associated with the Intranet role
  - To deny specific traffic for **Intranet subnets**, there needs to be an explicit rule to match

Troubleshooting

Reserved GBP Tag Troubleshooting

- Have a topology diagram ready with details involving the **FW** and **WAN Edge** Connections to the border VTEPs
- Recommended troubleshooting flow:

1. Check that the GBP border configurations are correctly applied
2. Check policy hitcounts on the border to verify traffic classes are matching
3. Verify “Intranet” and/or “Intranet” roles are present in packets forwarded to the access switches
4. Check policy hitcounts on Access switches for GBP policies
5. Check denied traffic is dropped at the Border VTEP
6. Check resources (TCAM exhaustion)



Troubleshooting Steps

1. Check that the GBP border configurations are correctly applied

- Ensure the isl, intranet and internet roles are present

```
Campus-Core-8360-A/B# show gbp role-mapping

GBP status : Disabled
GBP_ROLE                        GBP_ROLE_ID
-------------                   ---------------
camera                          110
default                         0
infra                           2
internet                        3
intranet                        4
isl                             5
printer                         100
signage                         120
```

```
Campus-Core-8360-A/B #show run gbp
gbp enable
gbp role camera 110
gbp role infra 2
gbp role internet 3
gbp role intranet 4
gbp role isl 5
gbp role printer 100
gbp role signage 120
gbp role intranet object-group ip Intranet_Subs
```

- Check prefixes assigned to the **"Intranet"** role

```
Campus-Core-8360-A/B# show object-group commands
object-group ip address Intranet_Subs
    vrf VRF1
   10 192.168.8.0/255.255.255.0
   20 192.168.9.0/255.255.255.0
   30 192.168.40.0/255.255.255.0
```

- Check the Role ACL configurations

```
Campus-Core-8360-A/B# show gbp role-access-list commands
gbp role access-list ip Intranet-ACLs_To_External
    10 permit printer 192.168.40.0/255.255.255.0 vrf VRF1 count
    20 permit signage 192.168.40.0/255.255.255.0 vrf VRF1 count
    30 permit signage 192.168.41.0/255.255.255.0 vrf VRF1 count
    40 deny camera 192.168.40.0/255.255.255.0 vrf VRF1 count
    apply gbp role-access-list ip Intranet-ACLs_To_External
```

Troubleshooting Steps

2. Check policy hitcounts on the border to verify traffic classes are matching

- We can see matches for the permitted and denied traffic at the border

```
Campus-Core-8360-A/B# show gbp role-access-list hitcounts ip Intranet-ACLs_To_External
Statistics for GBP_ACL Intranet-ACLs_To_External (ipv4):
     Matched Packets  Configuration
                  33  10 permit printer 192.168.40.0/255.255.255.0 vrf VRF1
                  18  20 permit signage 192.168.40.0/255.255.255.0 vrf VRF1
                  19  30 permit signage 192.168.41.0/255.255.255.0 vrf VRF1
                   5  40 deny camera 192.168.40.0/255.255.255.0 vrf VRF1
```

- Helpful to clear the counters to look at matches real-time

```
Campus-Core-8360-A/B# clear gbp role-access-list hitcounts ip Intranet-ACLs_To_External
```

Troubleshooting Steps

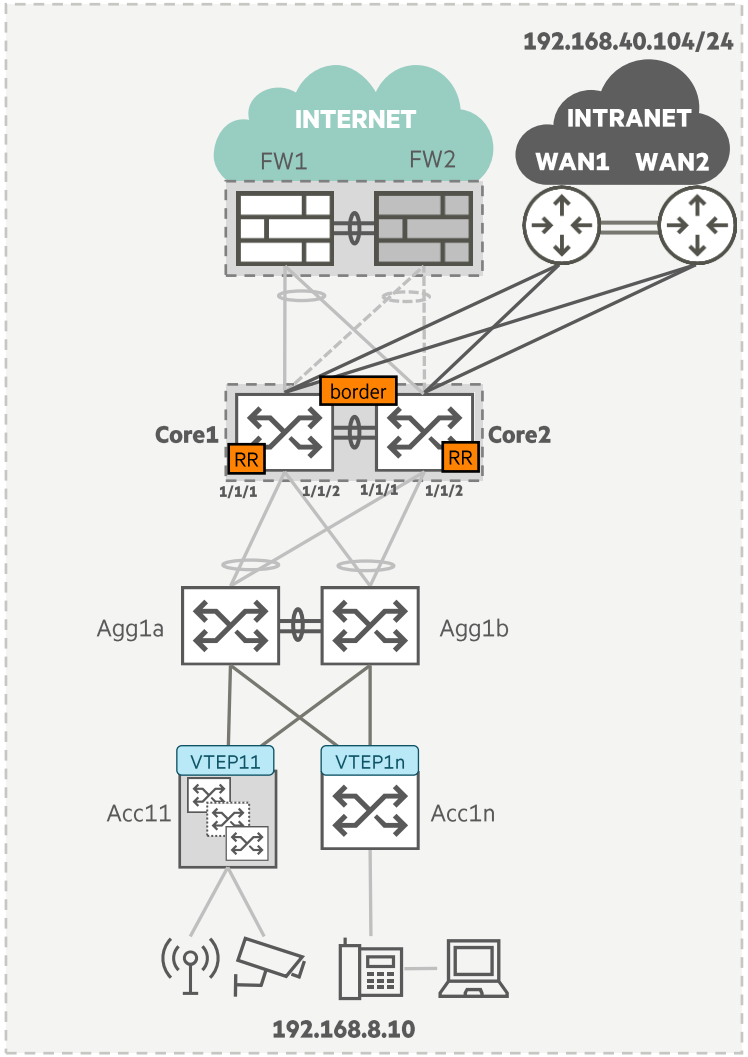
3. Verify “Intranet” an/or “Internet” roles are present in packets forwarded to access switches

- Packet capture ports egressing towards access switches

```
Campus-Core-8360-A/B# show mirror 1
 Mirror Session: 1
 Admin Status: enable
 Operation Status: enabled
 Source: vlan rx none
 Source: vlan tx none
 Source: interface 1/1/1 both
 Source: interface 1/1/2 both
 Destination: cpu
 Output Packets: 1679241
 Output Bytes: 219979655
```

- Verify the correct prefixes have the correct roles assigned

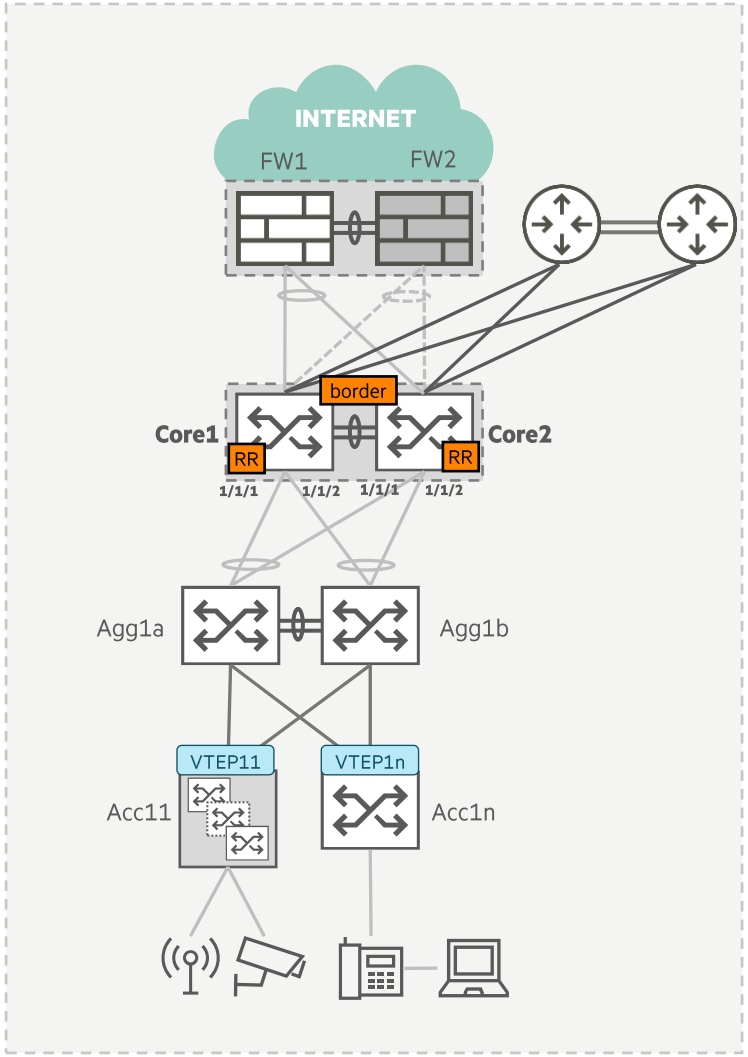
```
> Frame 16: 124 bytes on wire (992 bits), 124 bytes captured (992 bits)
> Ethernet II, Src: HewlettP_67:4f:80 (00:fd:45:67:4f:80), Dst: ArubaaHe_c5:71:80 (ec:02:73:c5:71:80)
> Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.12
> User Datagram Protocol, Src Port: 28716, Dst Port: 4789
v Virtual eXtensible Local Area Network
  > Flags: 0x8800, GBP Extension, VXLAN Network ID (VNI)
    Group Policy ID: 4
    VXLAN Network Identifier (VNI): 100001
    Reserved: 0
> Ethernet II, Src: HewlettP_67:4f:80 (00:fd:45:67:4f:80), Dst: 02:00:00:00:12:00 (02:00:00:00:12:00)
> Internet Protocol Version 4, Src: 192.168.40.104, Dst: 192.168.8.10
> Internet Control Message Protocol
```



Troubleshooting Steps

4. Check policy hitcounts on Access switches for GBP policies

```
Access VTEP11# show port-a gbp policy_icmp1 hitcounts

Port Access GBP Hit-Counts Details:
====================================

GBP Name   : policy_icmp1
GBP Type   : Local
GBP Status : Applied

SEQUENCE    CLASS                            TYPE     ACTION
----------- -------------------------------- -------- -----------------------
10          class_icmp1                      gbp-ipv4 permit
20          v6class_icmp1                    gbp-ipv6 permit
30          class_gbpmac1                    gbp-mac  permit


Class Name : class_icmp1
Class Type : gbp-ipv4

SEQUENCE    CLASS-ENTRY                                                HIT-COUNT
----------- ---------------------------------------------------------- -----------
10          match icmp internet camera count                          150
20          match icmp infra camera count                             5

Class Name : v6class_icmp1
Class Type : gbp-ipv6

SEQUENCE    CLASS-ENTRY                                                HIT-COUNT
----------- ---------------------------------------------------------- -----------
10          match icmpv6 internet camera count                        0

Class Name : class_gbpmac1
Class Type : gbp-mac

SEQUENCE    CLASS-ENTRY                                                HIT-COUNT
----------- ---------------------------------------------------------- -----------
10          match arp any camera count                                45
```



Troubleshooting Steps

5. Check denied traffic is dropped at the Border VTEP

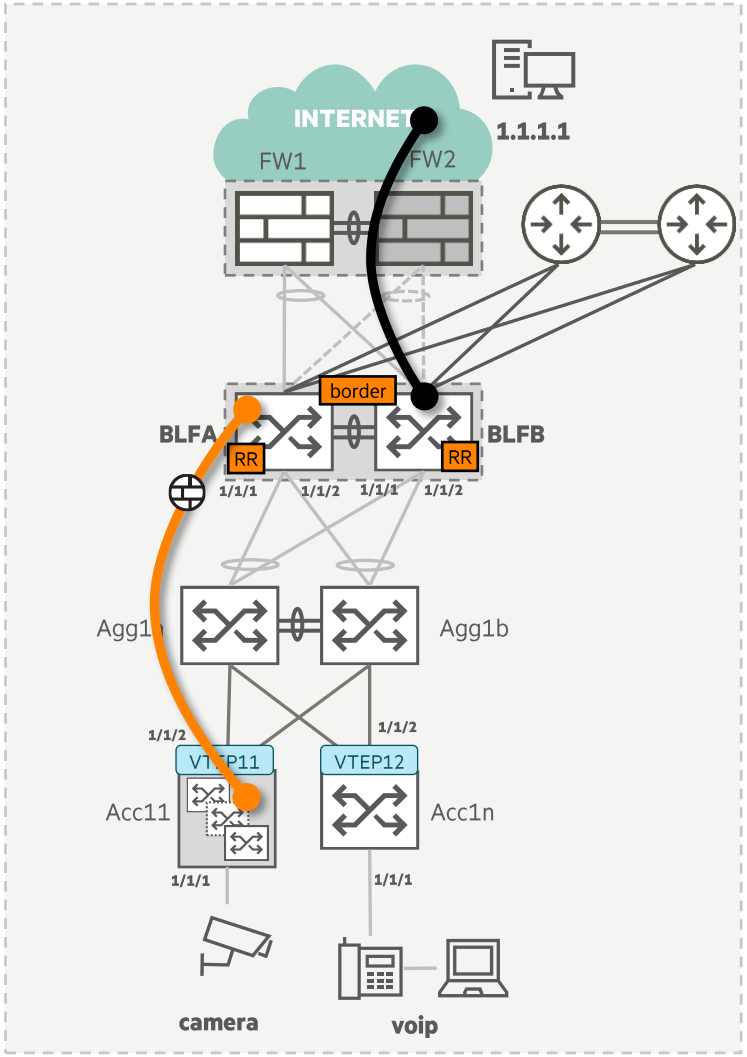
- Packet Captures
  - For example, **internet destination 1.1.1.1** is denied at the border
  - Packet captures at Border A/B confirm traffic does not egress ports 1/1/1 and 1/1/2 towards the access switches

```
Campus-Core-8360-A/B# show mirror 1
 Mirror Session: 1
 Admin Status: enable
 Operation Status: enabled
 Source: vlan rx none
 Source: vlan tx none
 Source: interface 1/1/1 both
 Source: interface 1/1/2 both
 Destination: cpu
 Output Packets: 1679241
 Output Bytes: 219979655
```

- Policy hitcounts
  - If source 1.1.1.1 is explicitly denied in a GBP role ACL with count action

```
gbp role access-list ip myinet-acl
    10 deny camera 1.1.1.1 count
```

  – Otherwise, the traffic will be silently discarded



Troubleshooting Steps

6. Check resources (TCAM) Exhaustion and event logs

- Event Logs / Debug Messages
  - show events -s err -c tcam
  - show events -s err -c policy
  - show events -s err -c port_access_gbp
  - show debug buffer module tcam
  - show debug bugger module policy
  - show debug buffer module gbpacl

```
8360(config)# show debug buffer module gbpacl
-----------------------------------------------------------------------------------------------------------------------------------
show debug buffer
-----------------------------------------------------------------------------------------------------------------------------------
2023-11-20:17:14:34.196043|ops-switchd|LOG_ERR|AMM|-|GBPACL|GBPACL|Unable to find the GBP ACL Global
2023-11-20:17:15:05.424772|ops-switchd|LOG_ERR|AMM|-|GBPACL|GBPACL|Unable to find the GBP ACL Global
2023-11-20:17:17:23.730060|ops-switchd|LOG_ERR|AMM|-|GBPACL|GBPACL|gbp_acl_populate_src_role_id Invalid source role name in GBP ACL Entry iot
```

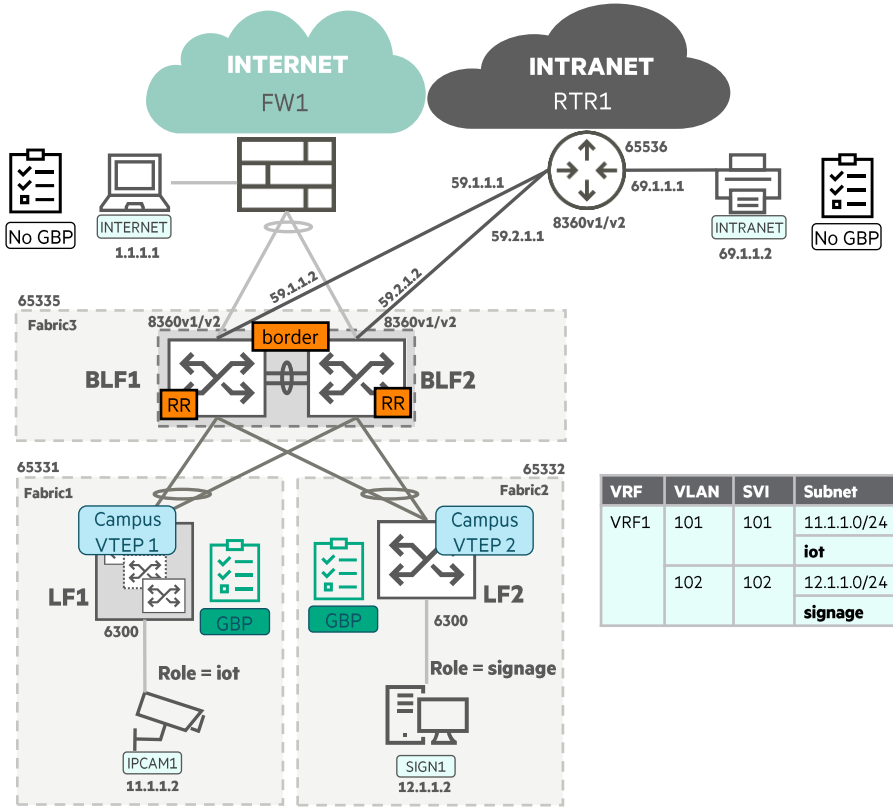
- Show resources

```
Resource Usage:

Mod  Description
         Resource                                    Used Reserved    Free
-------------------------------------------------------------------------------
1/1  Flex Lookup
         Ingress TCAM Entries                       14634    16384
     Total
         Ingress TCAM Entries                       14634    16384   49152
         Egress TCAM Entries                            0        0    8192
         Ingress Lookups                                0                9
         Ingress Flex Lookups                           1                0
         Egress Lookups                                 0                4
         Ingress Policers                               0             8191
         Egress Policers                                0             4095
```

Demo

Feature Demo

- Details
  - Multi-Fabric shared border
  - Mix of GBP, non-GBP traffic destinations
  - Internet / Intranet Destinations
  - ISL role for VSX deployments



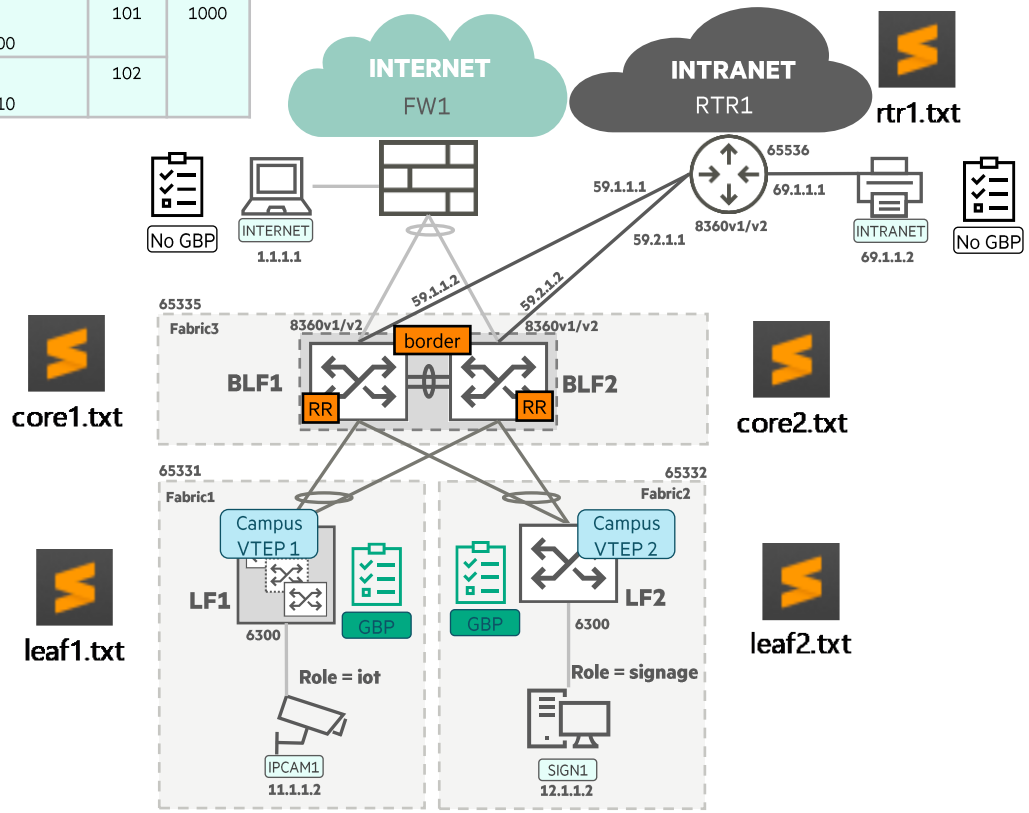
VRF	VLAN	SVI	Subnet	GBP Policy Id	L2VNI	L3VNI
VRF1	101	101	11.1.1.0/24		101	1000
			iot	100		
	102	102	12.1.1.0/24		102	
			signage	110		

Demo Configurations

Reserved GBP Tag for Internet Traffic

- Configurations from the demo are available as embedded text files from within this slide

VRF	VLAN	SVI	Subnet	GBP Policy Id	L2VNI	L3VNI
VRF1	101	101	11.1.1.0/24		101	1000
			iot	100		
	102	102	12.1.1.0/24		102	
			signage	110		



Thank you

aruba_switching_tme@hpe.com

© 2023 Hewlett Packard Enterprise Development LP