VNBT - VXLAN GBP

Presenters
- Daryl Wan
- Justin Noonan
Agenda

1. Overview
2. Use Cases
3. Details and Caveats
3. Configuration
4. Best Practices
5. Troubleshooting
7. Demo
8. Additional Resources
Overview
VXLAN Group Based Policy (GBP) Overview

- This feature enhances the Campus VXLAN - Virtual Network Based Tunneling (VNBT) solution
- 10.8 adds support for VXLAN GBP in VXLAN overlay networks

![VXLAN GBP Diagram]

- Supported on 6300/6400/8360
- Enables role based policies
  - Role based policies are no longer tied to IP addresses
  - Source based roles (e.g. employee or guest) are assigned to a user/device on ingress VTEP and would remain effective even if it authenticates at a different location, or is assigned to a different IP subnet
What is the difference between VXLAN GBP and GPO?

- They refer to the same thing
- From the expired IETF draft [https://www.ietf.org/archive/id/draft-smith-vxlan-group-policy-05.txt](https://www.ietf.org/archive/id/draft-smith-vxlan-group-policy-05.txt)
- GPO is mentioned in the title
- GBP is mentioned as the extension
VXLAN GBP
Use Cases
Micro-Segmentation Use Case

Users/Devices assigned to the same VLAN/subnet on a single switch

Users/Devices assigned to the same VLAN/subnet on different switches

- Role based policy can be created to prevent network connectivity between Employee and Guest roles

VLAN 200

Role = Employee

Role = Guest

VLAN 200

VLAN 200

Role = Employee

Role = Guest

VXLAN tunnel
Macro-Segmentation Use Case

**Users/Devices assigned to different VLANs/subnets/VRFs on a single switch**

- Role based policy can be created to prevent network connectivity between Employee and Guest roles

**Users/Devices assigned to different VLANs/subnets/VRFs on different switches**

- Role based policy can be created to prevent network connectivity between Employee and Guest roles

VLAN 200/VRF1

Role = Employee

VLAN 201/VRF2

Role = Guest
VXLAN GBP
Details
VXLAN GBP Details

- G bit indicates if Group Policy ID is being carried
- G bit = 0 = Group Policy ID IS NOT being carried

- D bit
- A bit
- D and A bit are not used by AOS-CX at this time
VXLAN GBP Details

- G bit indicates if Group Policy ID is being carried
- G bit = 1 = Group Policy ID IS being carried

```
Ethernet II, Src: ArubaHe_a5:9f:40 (b8:d4:e7:a5:9f:40), Dst: ArubaHe_b7:b5:00 (64:e8:81:b7:b5:00)
User Datagram Protocol, Src Port: 54284, Dst Port: 4789
Virtual eXtensible Local Area Network
  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
```

- Group Policy ID
Role Based Policy Details

- CLI uses GBP (Group Based Policy) keyword for Role Based Policy configuration
- gbp CLI is required on ingress/egress VTEPs, 1:1 mapping for role name to policy ID
- Works for traffic that is locally switched (source/destination on a single switch) or across multiple VTEPs for unicast/multicast/BUM traffic

Policy enforcement on a single switch

- Group policy # is applied on ingress VTEP after device authentication
- Role names (e.g. “Employee” or “Guest” are not sent between VTEPs)
- Role names are created locally on every required VTEP and mapped to Group Policy ID#
- Policy is enforced on egress VTEP

- Users/devices assigned to the same role = network connectivity allowed by default
- Users/devices assigned to different roles = network connectivity denied by default
Role Based Policy Details

- Users/devices are authenticated and assigned to roles via ClearPass (Aruba-User-Role VSA)

<table>
<thead>
<tr>
<th>Attributes:</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Name</td>
</tr>
<tr>
<td>Radius:Aruba</td>
<td>Aruba-User-Role</td>
</tr>
</tbody>
</table>

```
VNBT=Access(config)# show port-access clients

Port Access Clients

Status Codes: d device-mode, c client-mode, m multi-domain

<table>
<thead>
<tr>
<th>Port</th>
<th>MAC-Address</th>
<th>Onboarding Method</th>
<th>Status</th>
<th>Role</th>
<th>Device Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>c 1/1/1</td>
<td>cc:bb:bb:00:00:01</td>
<td>mac-auth</td>
<td>Success</td>
<td>Ultrasound</td>
<td></td>
</tr>
<tr>
<td>c 1/1/51</td>
<td>aa:aa:aa:00:00:01</td>
<td>mac-auth</td>
<td>Success</td>
<td>Employee</td>
<td></td>
</tr>
<tr>
<td>c 1/1/51</td>
<td>aa:bb:cc:00:00:01</td>
<td>mac-auth</td>
<td>Success</td>
<td>Guest</td>
<td></td>
</tr>
<tr>
<td>c 1/1/51</td>
<td>cc:aa:aa:00:00:01</td>
<td>mac-auth</td>
<td>Success</td>
<td>Maintenance</td>
<td></td>
</tr>
<tr>
<td>c 1/1/52</td>
<td>cc:cc:cc:00:00:01</td>
<td>mac-auth</td>
<td>Success</td>
<td>Heart-Monitor</td>
<td></td>
</tr>
</tbody>
</table>
```

- Assigned role name needs to match in CLI

```
gbp role Employee 100
gbp role Heart-Monitor 200
gbp role Maintenance 400
gbp role Ultrasound 300

VNBT=Access(config)# show port-access role name Employee

Role Information:

Name : Employee
Type : local
VXLAN GBP / Role Based Policy Caveats

- Source roles must be created at ingress VTEP
- Source and destination roles must be created at egress VTEP

- Only 8K Tags
  - Currently supports only 13-bits in the tag field as opposed to 16-bits defined in the IETF draft
  - Upper 3 bits of the tag from inbound GBP tagged traffic are ignored by AOS-CX switches

- 8360 does not support role-based policies, it can only be used as Stub VTEP to relay GBP tags
- MAC based authentication (6300/6400) is required to assign roles to users/devices and implement role-based policies

- No VSX at the access
  - VSX can be used towards infrastructure devices, not towards authenticated users/devices that are dual homed

- Single default tag
  - All unknown traffic and roles without a GBP tag use the default tag of 0 and is permitted at the egress VTEP (can't be denied with GBP policy)
  - CPU snooped/generated packets will always be sent with role 0

- Only local user roles are supported for GBP-based policy

- Role can only exist in 1 VLAN – can’t have the same role name exist across multiple VLANs on a single switch

- Policy to allow ARP on VTEPs are required – traffic is denied by default between different user roles using GBP

- Not currently supported:
  - DHCP snooping with GBP
  - COA
VXLAN GBP / Role Based Policy Caveats

Multiple Roles behind the same port – multicast traffic limitation
- If both “permit” clients and “deny” clients are connected to the same exit port on the egress VTEP towards a hub, the GBP ACL will let multicast traffic out of the port, ignoring the presence of “deny” clients. The downstream hub/non-learning switch broadcasts it to both Guest and Finance roles/devices.

![Diagram showing VXLAN GBP / Role Based Policy Caveats]

**Intention**
- Ingress VTEP: VLAN 200 (Role = Employee)
- VXLAN tunnel: VNI 200
- Egress VTEP: VLAN 200 (Role = Guest)
- GBP ACL: deny
- L2 switch: Role = Finance

**Current Implementation**
- Ingress VTEP: VLAN 200 (Role = Employee)
- VXLAN tunnel: VNI 200
- Egress VTEP: VLAN 200 (Role = Guest)
- GBP ACL: deny
- L2 switch: Role = Finance
Configuration
Access VTEP (Distributed L3 gateway) Configuration

vrf VRF1
  rd 192.168.0.3:1
  route-target export 65100:1 evpn
  route-target import 65100:1 evpn
  !
  vrf 1,200,202
  virtual-mac 02:00:00:00:03:00
  evpn
  vlan 200
  rd auto
  route-target export auto
  route-target import auto
  redistribute host-route
  vlan 202
  rd auto
  route-target export auto
  route-target import auto
  redistribute host-route
  !
  interface loopback 0
  ip address 192.168.0.3/32
  ip ospf 1 area 0.0.0.0
  !
  interface vlan 200
  vrf attach VRF1
  ip address 192.168.200.1/24
  active-gateway ip mac 12:00:00:00:01:00
  active-gateway ip 192.168.200.1
  interface vlan 202
  vrf attach VRF1
  ip address 192.168.202.1/24
  active-gateway ip mac 12:00:00:00:01:00
  active-gateway ip 192.168.202.1

interface vxlan 1
  source ip 192.168.0.3
  no shutdown
  vni 200
  vlan 200
  vni 202
  vlan 202
  vni 100001
  vrf VRF1
  routing
  !
  router ospf 1
  router-id 192.168.0.3
  area 0.0.0.0
  router bgp 65100
  bgp router-id 192.168.0.3
  no bgp fast-external-fallover
  neighbor 192.168.0.1 remote-as 65100
  neighbor 192.168.0.1 update-source loopback 0
  address-family 12vpn evpn
  neighbor 192.168.0.1 activate
  neighbor 192.168.0.1 send-community extended
  exit-address-family
  !
  vrf VRF1
  address-family ipv4 unicast
  redistribute connected
Access VTEP [Group Based Policy (GBP) + Colorless Port] Configuration

gbp enable
gbp role Employee 100
gbp role Heart-Monitor 200
gbp role Maintenance 400
gbp role Ultrasound 300
class gbp-ip block-maintenance
  10 match any Maintenance Ultrasound count
class gbp-ip blocktcp20
  10 match tcp Heart-Monitor Ultrasound eq ftp-data count
class gbp-ip employee
  10 match any Employee count
class gbp-ip heartmon
  10 match any Heart-Monitor count
class gbp-ip maintenance
  10 match any any Maintenance count
class gbp-ip ultrasound
  20 match udp any Ultrasound eq 5004 count
class gbp-ip ultrasound-allowall
  10 match any any Ultrasound count
class gbp-mac employee
  10 match any Employee arp count
class gbp-mac heartmon
  30 match any Heart-Monitor arp count
class gbp-mac maintenance
  10 match any any Maintenance arp count
class gbp-mac ultrasound
  10 match any Ultrasound arp count

GBP Role to ID Mapping

MAC and IP Classes defined to match traffic source and destination

Policy configured to provide action statements for classifiers

Policy associated to user role

port-access gbp employee
  10 class gbp-mac employee
  20 class gbp-ip employee
port-access gbp heartmon
  20 class gbp-ip heartmon
port-access gbp maintenance
  10 class gbp-mac maintenance
port-access gbp ultrasound
  20 class gbp-ip ultrasound
port-access gbp maintenance
  10 class gbp-mac maintenance
port-access gbp ultrasound
  20 class gbp-ip ultrasound
  21 class gbp-ip block-maintenance action drop
22 class gbp-ip blocktcp20 action drop
  25 class gbp-ip ultrasound-allowall
  30 class gbp-mac ultrasound
port-access role Employee
  associate gbp employee
dev vlan access name user
port-access role Guest
  vlan access name user
port-access role Heart-Monitor
  associate gbp heartmon
dev vlan access name device
port-access role Maintenance
  associate gbp maintenance
dev vlan access name user
port-access role Ultrasound
  associate gbp ultrasound
dev vlan access name device
aaa authentication port-access mac-auth
  enable
interface 1/1/1
  no shutdown
  no routing
dev vlan access 1
aaa authentication port-access client-limit 10
aaa authentication port-access mac-auth
  enable
Best Practices
Best Practices

- Ensure “enable gbp” is configured on VTEPs
- Use upper case for role – aesthetic purposes
- Use lower case for classes/policy – easier to type if needing to make quick changes
- Name Classes and Policies similar to role name if possible – makes it easier for troubleshooting

```plaintext
gbp role Ultrasound 300

class gbp-ip block-maintenance
  10 match any Maintenance Ultrasound count

class gbp-ip blocktcp20
  10 match tcp Heart-Monitor Ultrasound eq ftp-data count

class gbp-ip ultrasound
  20 match udp any Ultrasound eq 5004 count

class gbp-ip ultrasound-allowall
  10 match any any Ultrasound count

port-access gbp ultrasound
  20 class gbp-ip ultrasound
  21 class gbp-ip block-maintenance action drop
  22 class gbp-ip blocktcp20 action drop
  25 class gbp-ip ultrasound-allowall
  30 class gbp-mac ultrasound

port-access role Ultrasound
  associate gbp ultrasound
  vlan access name device
```
VXLAN GBP Troubleshooting

- Troubleshooting flow

  Check underlay network reachability and VXLAN tunnels are up between VTEPs
  Check VTEP connectivity to Clearpass?
  Check desired roles and policies are created
  Check authenticated users/devices are assigned to correct roles
  Check GBP tags are exchanged between VTEPs

  Check role-based policy works as expected
  Check traffic flows are using the appropriate traffic classes (ensure count command is in class statement)

- debug gbp – Example shows port removed and added to the GBP policy

  2021-07-22:17:03:32.328515|ops-switchd|LOG_DEBUG|MSTR|1|GBPFR|GBPFR ASIC|gbp_delete_port_from_all_roles|Remove port 1/1/52 from filter index 14
  2021-07-22:17:03:22.255558|ops-switchd|LOG_DEBUG|MSTR|1|GBPFR|GBPFR ASIC|gbp_add_port_to_all_filters|Add port 1/1/52 to filter index 14
Check underlay network reachability and VXLAN tunnel between VTEPs

- Ensure tunnel source/destination IPs are correctly advertised in the underlay network
  - e.g. “sh ip route”, test pings using loopback source/destination IPs
  - Fix underlay connectivity issues if discovered

- If there are no underlay network issues
  - Validate VXLAN tunnels

```
VNBT=Access(config)# show interface vxlan vteps
Source           Destination      Origin       Status                VNI       Routing   VLAN  VRF
----------------- ----------------- ------------ ------------- -------------- ------- ------ -----
192.168.0.3      192.168.0.1     evpn           operational       58        disabled  58  --
192.168.0.3      192.168.0.1     evpn           operational       202       disabled  202 --
192.168.0.3      192.168.0.1     evpn           operational      100001    enabled  --  VRF1
```

- If EVPN tunnel is down
  - Ensure correct EVPN configs are used
Check VTEP connectivity to Clearpass

- Ensure that the authenticating switch has connectivity to ClearPass

```
VNBT> show running-config | include radius
radius-server retries 3
radius-server host 10.5.8.12 tls vrf VRF1
tls vrf VRF1
cipher text
radius server host fc00:10:5:8::12 key ciphertext
AQBapdAz4irjSK61Zg/CFArsNYWWbn1L0bqDD/v9SHleMQ6ABQAAADY261iu vrf VRF1
aaa group server radius radsec
dyn-authorization enable
debug radius all
ip source-interface radius 10.5.8.19
ip source-interface radius interface loopback10 vrf VRF1
ipv6 source-interface radius interface loopback10 vrf VRF1
```

```
VNBT> ping 10.5.8.12 vrf VRF1
PING 10.5.8.12 (10.5.8.12) 100(128) bytes of data.
108 bytes from 10.5.8.12: icmp_seq=1 ttl=62 time=0.527 ms
108 bytes from 10.5.8.12: icmp_seq=2 ttl=62 time=0.538 ms
108 bytes from 10.5.8.12: icmp_seq=3 ttl=62 time=0.464 ms
108 bytes from 10.5.8.12: icmp_seq=4 ttl=62 time=0.452 ms
108 bytes from 10.5.8.12: icmp_seq=5 ttl=62 time=0.482 ms
--- 10.5.8.12 ping statistics ---
 5 packets transmitted, 5 received, 0% packet loss, time 4086ms
rtt min/avg/max/mdev = 0.452/0.492/0.538/0.034 ms
```
Check desired roles and policies are created

List Roles

VNBT-Access(config)# show port-access role

Role Information:
Attributes overridden by RADIUS are prefixed by '*'.

Name : Employee
Type  : local

----------------------------------------------
Reauthentication Period :
Cached Reauthentication Period :
Authentication Mode :
Session Timeout :
Client Inactivity Timeout :
Description :
Gateway Zone :
UBT Gateway Role :
UBT Gateway Clearpass Role :
Access VLAN :
Native VLAN :
Allowed Trunk VLANs :
Access VLAN Name : user
Native VLAN Name :
Allowed Trunk VLAN Names :
VLAN Group Name :
MTU :
QOS Trust Mode :
STP Administrative Edge Port :
PoE Priority :
PVLAN Port Type :
Captive Portal Profile :
Policy :
GBP :
Device Type :

List GBP Policy

VNBT-Access(config)# show port-access gbp

Port Access GBP User Configured Policy Details:

GBP Name   : employee
GBP Type   : Local
GBP Status : Applied

<table>
<thead>
<tr>
<th>SEQUENCE</th>
<th>CLASS</th>
<th>TYPE</th>
<th>ACTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>employee</td>
<td>gbp-mac</td>
<td>permit</td>
</tr>
<tr>
<td>20</td>
<td>employee</td>
<td>gbp-ipv4</td>
<td>permit</td>
</tr>
</tbody>
</table>

GBP Name   : heartmon
GBP Type   : Local
GBP Status : Applied

<table>
<thead>
<tr>
<th>SEQUENCE</th>
<th>CLASS</th>
<th>TYPE</th>
<th>ACTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>20</td>
<td>heartmon</td>
<td>gbp-ipv4</td>
<td>permit</td>
</tr>
<tr>
<td>30</td>
<td>heartmon</td>
<td>gbp-mac</td>
<td>permit</td>
</tr>
</tbody>
</table>
Check authenticated users/devices are assigned to correct roles

- Authenticated users/devices should be mapped to desired role
- Check authentication configs, clearpass etc if expected output is not seen

### VNBT Access(config)# show port-access clients

<table>
<thead>
<tr>
<th>Port</th>
<th>MAC-Address</th>
<th>Onboarding Method</th>
<th>Status</th>
<th>Role</th>
<th>Device Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>c 1/1/1</td>
<td>cc:bb:bb:00:00:01</td>
<td>mac-auth</td>
<td>Success</td>
<td>Ultrasound</td>
<td></td>
</tr>
<tr>
<td>c 1/1/51</td>
<td>aa:aa:aa:00:00:01</td>
<td>mac-auth</td>
<td>Success</td>
<td>Employee</td>
<td></td>
</tr>
<tr>
<td>c 1/1/51</td>
<td>aa:bb:cc:00:00:01</td>
<td>mac-auth</td>
<td>Success</td>
<td>Guest</td>
<td></td>
</tr>
<tr>
<td>c 1/1/51</td>
<td>cc:aa:aa:00:00:01</td>
<td>mac-auth</td>
<td>Success</td>
<td>Maintenance</td>
<td></td>
</tr>
<tr>
<td>c 1/1/52</td>
<td>cc:cc:cc:00:00:01</td>
<td>mac-auth</td>
<td>Success</td>
<td>Heart-Monitor</td>
<td></td>
</tr>
</tbody>
</table>
Check GBP tags are exchanged between VTEPs

- Port mirroring and packet captures should be used
- Check source GBP tags sent in both directions
- If expected tags are not seen, role based policies will not work
Check GBP policy works as expected

- Check class counters in policy

VNBT-Access(config)# show port-access gbp ultrasound hitcounts

Port Access GBP Hit-Counts Details:
======================================
GBP Name   : ultrasound
GBP Type   : Local
GBP Status : Applied

<table>
<thead>
<tr>
<th>SEQUENCE</th>
<th>CLASS</th>
<th>TYPE</th>
<th>ACTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>20</td>
<td>ultrasound</td>
<td>gbp</td>
<td>ipv4 permit</td>
</tr>
<tr>
<td>21</td>
<td>block-maintenance</td>
<td>gbp</td>
<td>ipv4 drop</td>
</tr>
<tr>
<td>22</td>
<td>blocktcp20</td>
<td>gbp</td>
<td>ipv4 drop</td>
</tr>
<tr>
<td>25</td>
<td>ultrasound-allowall</td>
<td>gbp</td>
<td>ipv4 permit</td>
</tr>
<tr>
<td>30</td>
<td>ultrasound</td>
<td>gbp</td>
<td>mac permit</td>
</tr>
</tbody>
</table>

Class Name : ultrasound
Class Type : gbp-ipv4

<table>
<thead>
<tr>
<th>SEQUENCE</th>
<th>CLASS-ENTRY</th>
<th>HIT-COUNT</th>
</tr>
</thead>
<tbody>
<tr>
<td>20</td>
<td>match udp</td>
<td>0</td>
</tr>
</tbody>
</table>

Class Name : block-maintenance
Class Type : gbp-ipv4

<table>
<thead>
<tr>
<th>SEQUENCE</th>
<th>CLASS-ENTRY</th>
<th>HIT-COUNT</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>match any</td>
<td>1005</td>
</tr>
</tbody>
</table>
Use Case 1
- Demo micro segmentation (same VLAN 202) on the same switch with both unicast and BUM traffic

Use Case 2
- Demo micro segmentation (same VLAN 202) between static/EVPN VXLAN tunnels with unicast traffic

Use Case 3
- Role without GBP ID

Use Case 4
- Demo macro segmentation (different VLANs 200, 202) on same switch

Use Case 5
- Demo macro segmentation (different VLANs 201-202) between static/EVPN VXLAN tunnels
Resources
Feature/Solution References

– RFCs

https://www.ietf.org/archive/id/draft-smith-vxlan-group-policy-05.txt
Thank you

daryl.wan@hpe.com
justin.noonan@hpe.com