Hewlett Packard Enterprise

HPE aruba networking

AOS-CX 10.13 Update: Reflexive Policy

- **Reflexive Port Access Policy**
- **Reflexive Group Based Policy**

Shobana Nandakumar , Technical Marketing Engineer

November 2023

Acronyms

PAP – **P**ort **A**ccess **P**olicy

GBP – **G**roup **B**ased **P**olicy

ABP – **A**pplication **B**ased **P**olicy

TCAM – **T**ernary **C**ontent **A**ddressable **M**emory

IPFM – **IP F**low **M**anager

C2S – **C**lient **t**o **S**erver

S2C – **S**erver to **C**lient

VSA – **V**endor **S**pecific **A**ttribute

LUR – **L**ocal **U**ser **R**ole

DUR – **D**ownloadable **U**ser **R**ole

DoS – **D**enial **o**f **S**ervice

DDoS – **D**istributed **D**enial **o**f **S**ervice

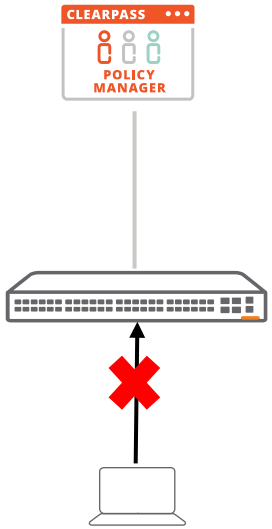
CPS – **C**onnections **P**er **S**econd

R2R – **R**ole **t**o **R**ole

Overview

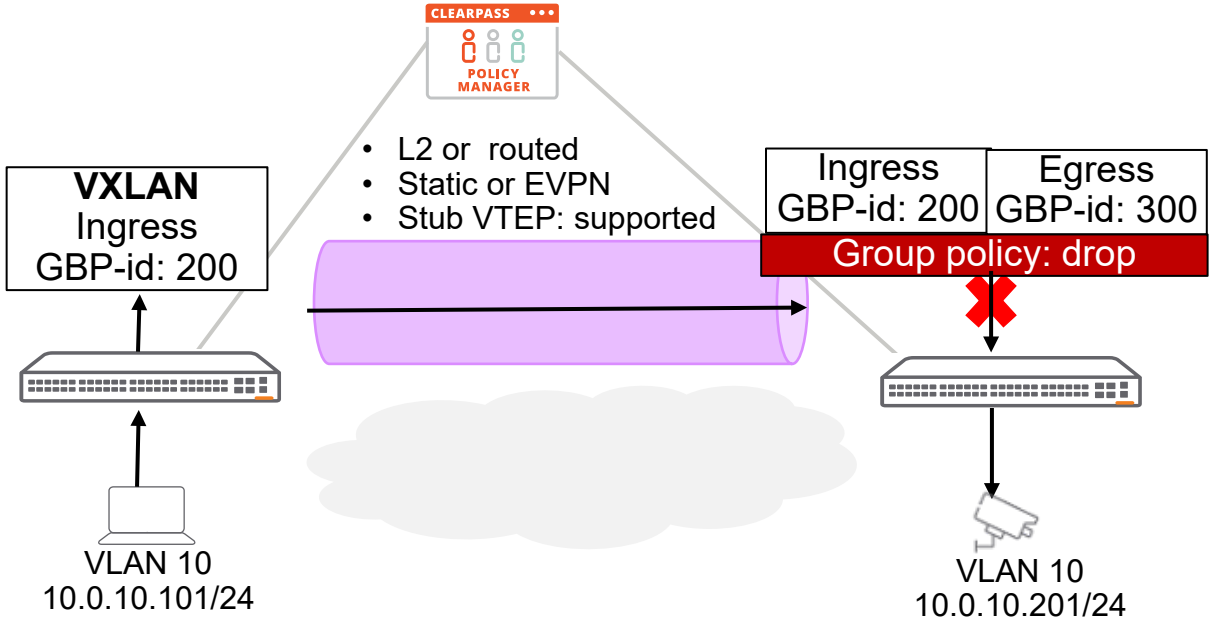
Secure Policy

- **Port Access Policy (PAP)**
  - Set of Rules to restrict or alter the passage of ingress traffic from clients onboarding to a switch that has port access security enabled.
  - Achievable using – LUR/DUR/VSA



Drop Incoming UDP traffic from Client

- **Group Based Policy (GBP)**
  - **Role** Based Policy. Segment user traffic in a network by grouping the users into roles based on user authentication at the source or ingress VXLAN tunnel endpoint (VTEP).
  - Achievable using – LUR/DUR*



Role: Employee = 200

Role: Surveillance = 300

*DUR – Technically works, but no official validation

Reflexive Policy Overview

- **Prior to 10.13 –**
  - Secure Policies restrict the traffic flow in ingress (PAP) or egress (GBP) for the authenticated clients.
  - Reverse traffic that belongs to the same flow will require a separate policy entry in the opposite direction.

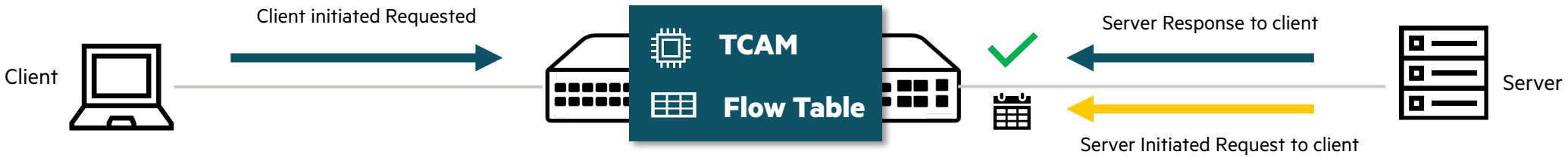
    – Increases configuration complexity and prone to errors.

    – Unscalable as requires additional configuration.

- **Enhancements in 10.13 –**
  - With Reflexive Policy support, switch maintains flow table for permitted traffic based on policy, and automatically allows return traffic for permitted flows.
  - Enables the switch to allow a packet destined to the authenticated client only if the flow is learnt and initiated by the client.
  - Reflexive Policy – PAP and GBP
  - Part of **CX Advanced Feature-Pack**
  - IPv4 and IPv6 Unicast traffic only. UDP/TCP based applications (i.e. no ICMP yet)
  - **Supported platforms** – 6400v2 and 6300.
  - Achievable using LUR and DUR (Reflexive PAP).

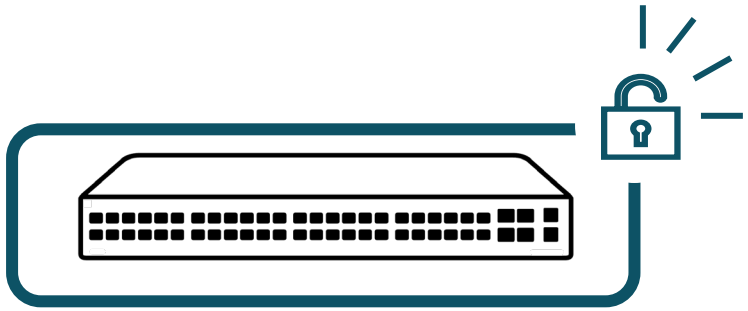
Reflexive Policy Characteristics

- The **Reflect** action enables the switch to allow the return packet destined to the client **only if** the flow was initiated by the client and got learned/programmed in the switch flow table.



- Reflexive action associated to a matching class entry is always a "**permit**".
- SRC/DST IP and SRC/DST Port are tracked in the ASIC flow table, to allow the return flow in the TCAM.
- Supported protocols: IPv4/IPv6, TCD/UDP, unicast only.
- Available for **P**ort-**A**ccess-**P**olicy and **G**roup-**B**ased-**P**olicy.
- In a given Reflexive Policy, **reflect** action associated to at least one class entry creates "permit" rules for reverse flows of policy classes where reflect action is not applied.

Why Reflexive Policy part of CX Advanced Feature-Pack ?

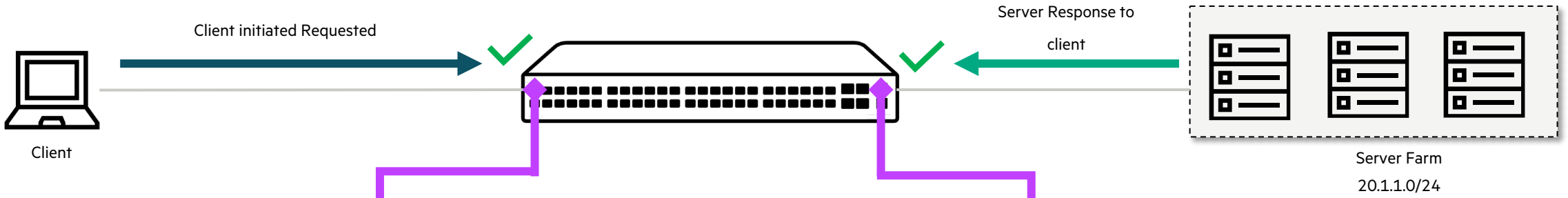


Advanced Security and Threat Intelligence

Use Cases

Operational Simplification of Secure Policy Deployment

Prior to 10.13 -



Policy applied to client

```
class ip tcp_sample_class_client
    10 match tcp any 20.1.1.10 eq ssh
    20 match tcp any 20.1.1.10 eq telnet
    30 match tcp any 20.1.1.20 eq ssh
    40 match tcp any 20.1.1.20 eq telnet
    50 match tcp any 20.1.1.30 eq ssh
    60 match tcp any 20.1.1.30 eq telnet
class ip udp_sample_class_client
    10 match udp any 20.1.1.10 eq snmp
    20 match udp any 20.1.1.20 eq snmp
    30 match udp any 20.1.1.30 eq snmp
port-access policy sample_client_policy
    10 class ip udp_sample_class_client
    20 class ip tcp_sample_class_client
port-access role client
    associate policy sample_client_policy
    vlan access 10
```

Increases configuration complexity and prone to errors.

Unscalable as requires additional cumbersome configuration.

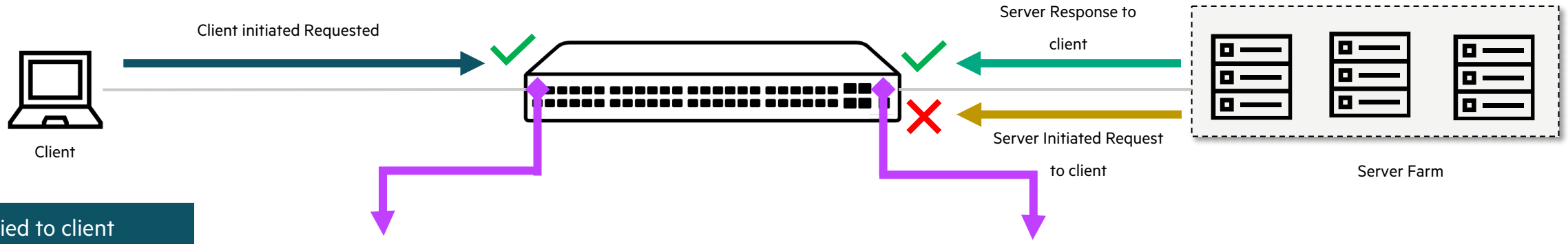
Policy applied to Server

```
class ip tcp_sample_class_server
    10 match tcp 20.1.1.10 eq ssh any
    20 match tcp 20.1.1.10 eq telnet any
    30 match tcp 20.1.1.20 eq ssh any
    40 match tcp 20.1.1.20 eq telnet any
    50 match tcp 20.1.1.30 eq ssh any
    60 match tcp 20.1.1.30 eq telnet any
class ip udp_sample_class_server
    10 match udp 20.1.1.10 eq snmp any
    20 match udp 20.1.1.20 eq snmp any
    30 match udp 20.1.1.30 eq snmp any
port-access policy sample_server_policy
    10 class ip udp_sample_class_server
    20 class ip tcp_sample_class_server
Interface <physical/lag/vlan>
    apply policy sample_server_policy
```

Operational Simplification of Secure Policy Deployment

Example Workflow with Reflexive PAP

10.13 Onwards -



Policy applied to client

```
class ip tcp_sample_class_client
    10 match tcp any 20.1.1.10 eq ssh
    20 match tcp any 20.1.1.10 eq telnet
    30 match tcp any 20.1.1.20 eq ssh
    40 match tcp any 20.1.1.20 eq telnet
    50 match tcp any 20.1.1.30 eq ssh
    60 match tcp any 20.1.1.30 eq telnet
class ip udp_sample_class_client
    10 match udp any 20.1.1.10 eq snmp
    20 match udp any 20.1.1.20 eq snmp
    30 match udp any 20.1.1.30 eq snmp
port-access policy sample_client_policy
    10 class ip udp_sample_class_client action reflect
    20 class ip tcp_sample_class_client action reflect
port-access role client
    associate policy sample_client_policy
    vlan access 10
```

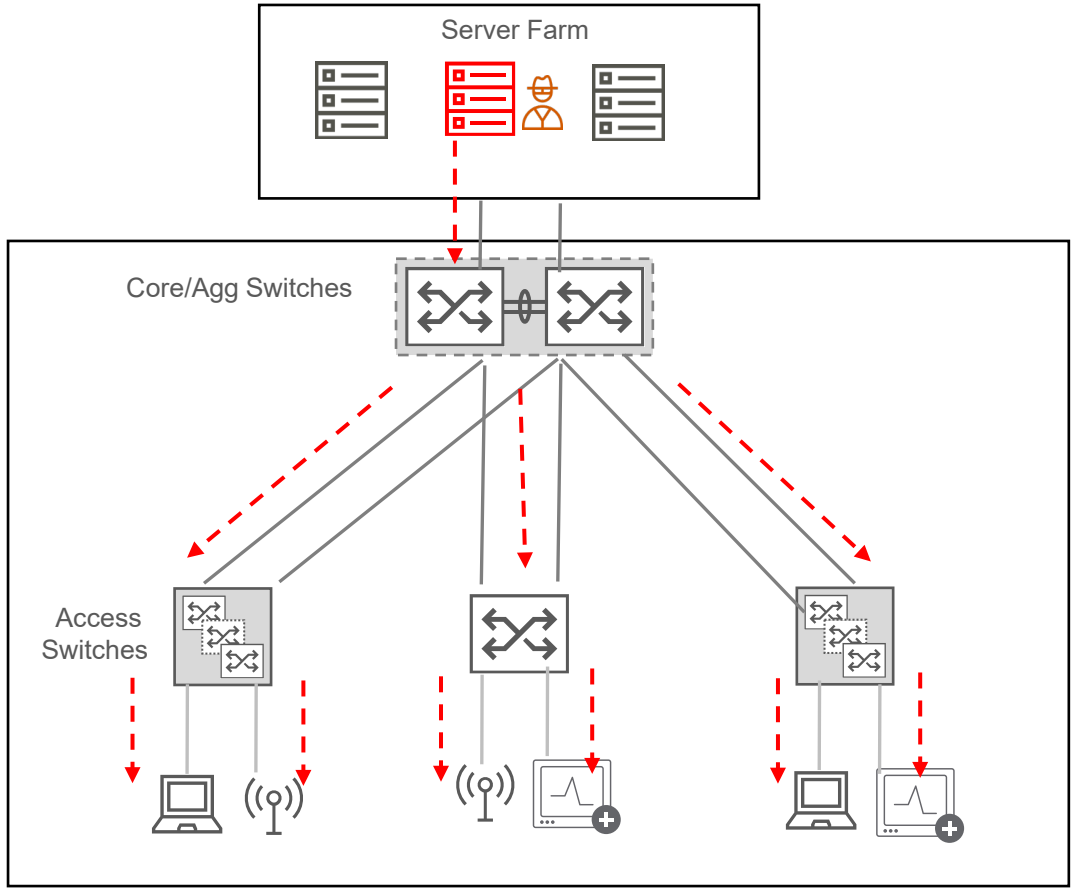
Ease of Management – No Server-side Policy configuration and Capable of handling Server connected interface movements

Scalable with much less configurations.

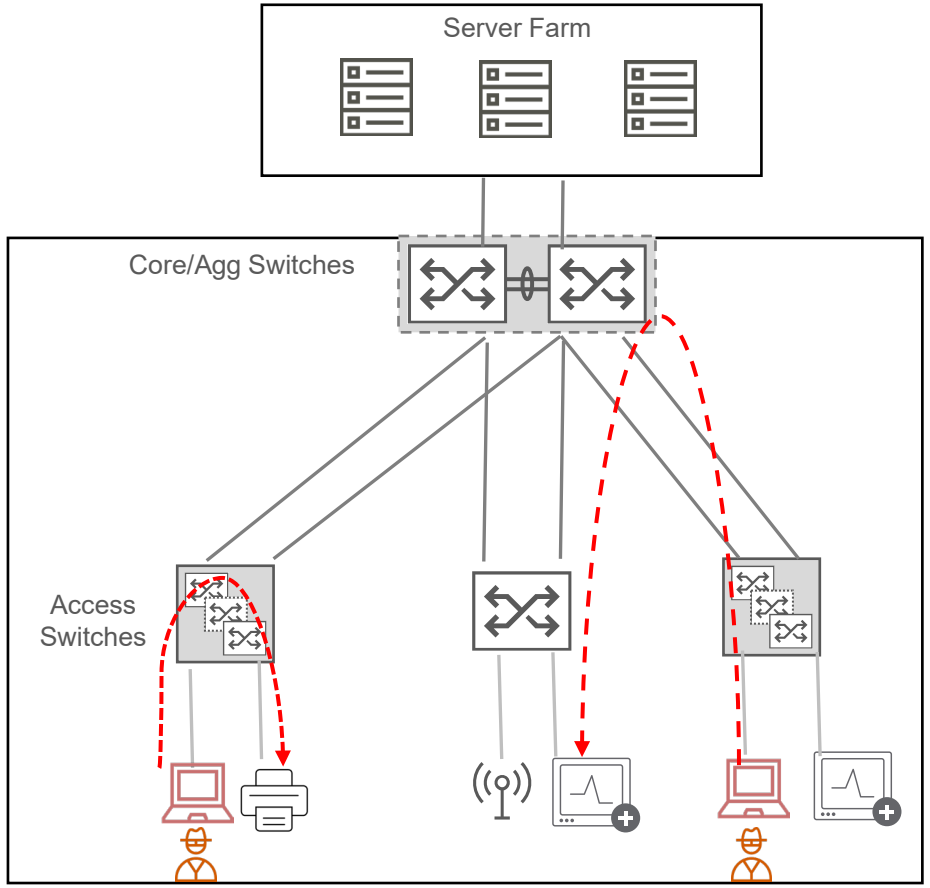
Cybersecurity Attacks - DoS/DDoS/Worm Propagation

Illegitimate Flows

Vertical Propagation



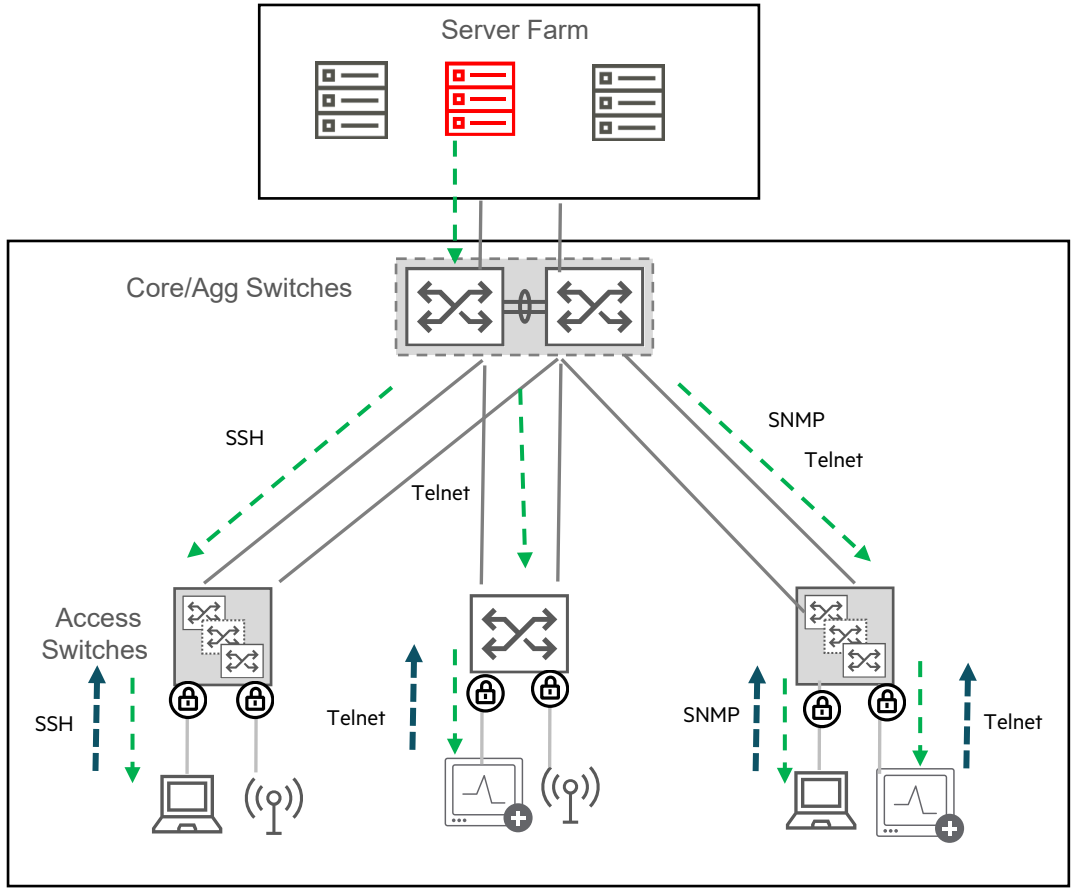
Horizontal Propagation



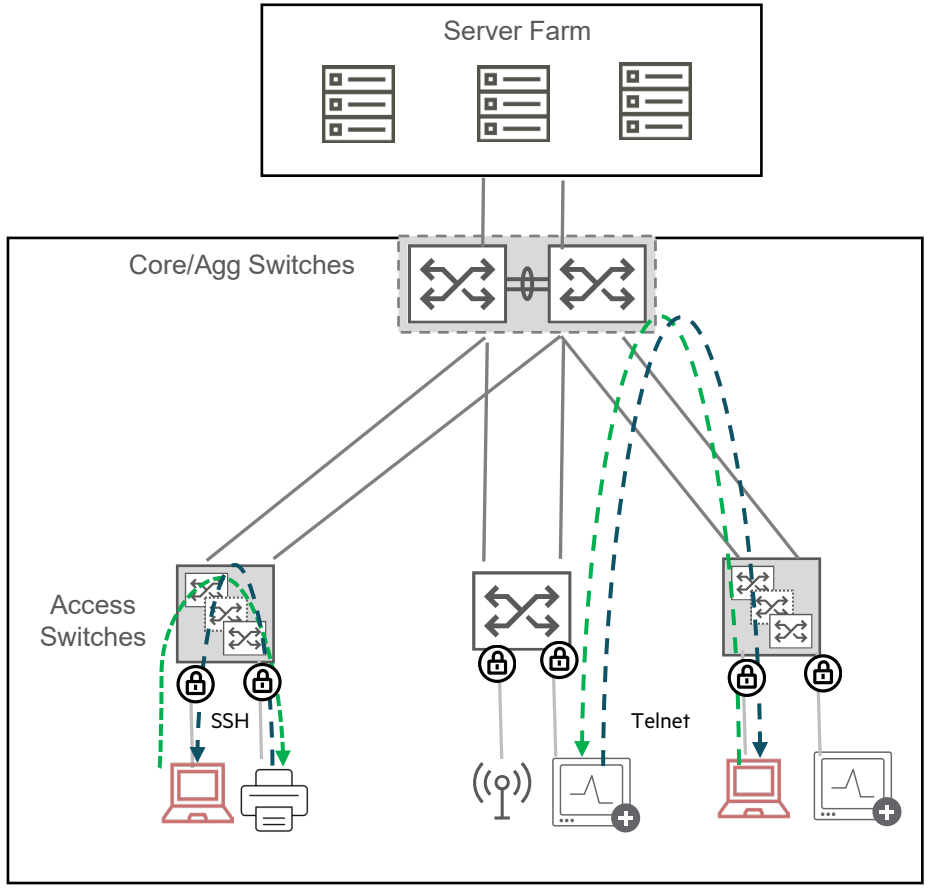
Prevention against cybersecurity attacks

Legitimate Flows

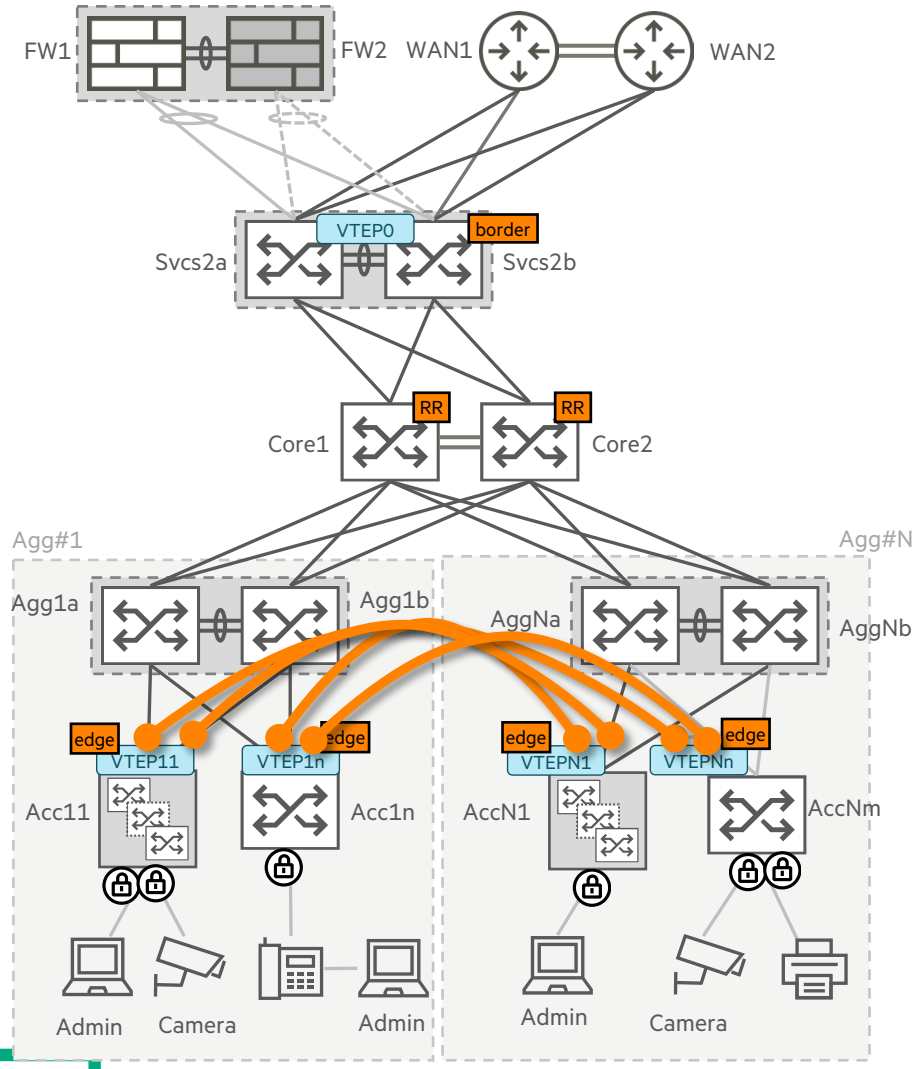
Vertical Propagation



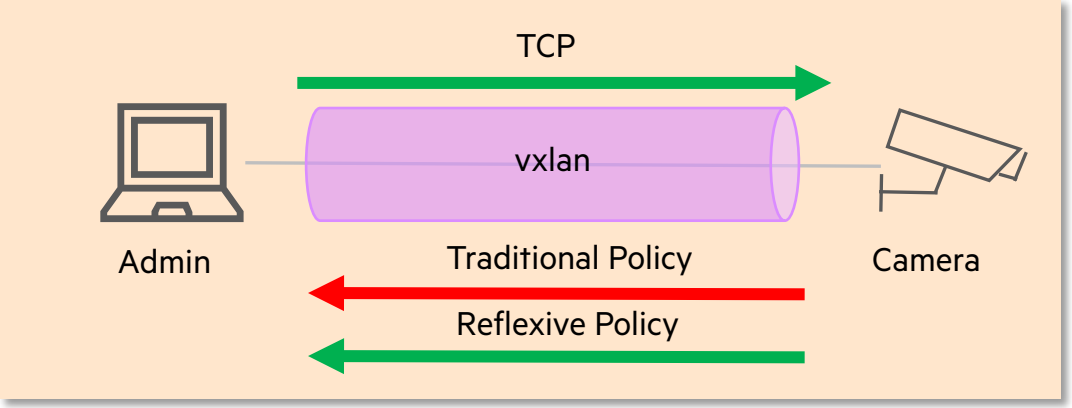
Horizontal Propagation



Micro & Macro Segmentation - GBP

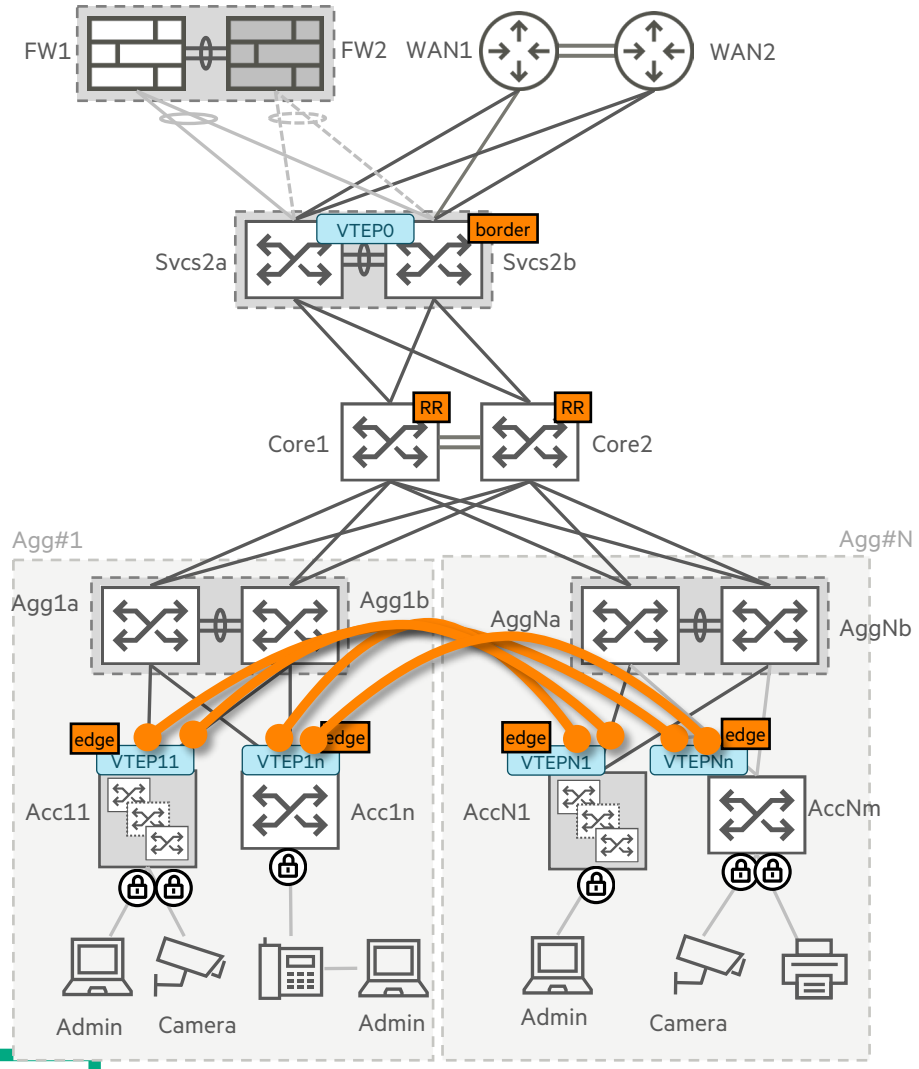


Source	Destination	
	Admin	Camera
Admin	✓	✓
Camera	✗	✓

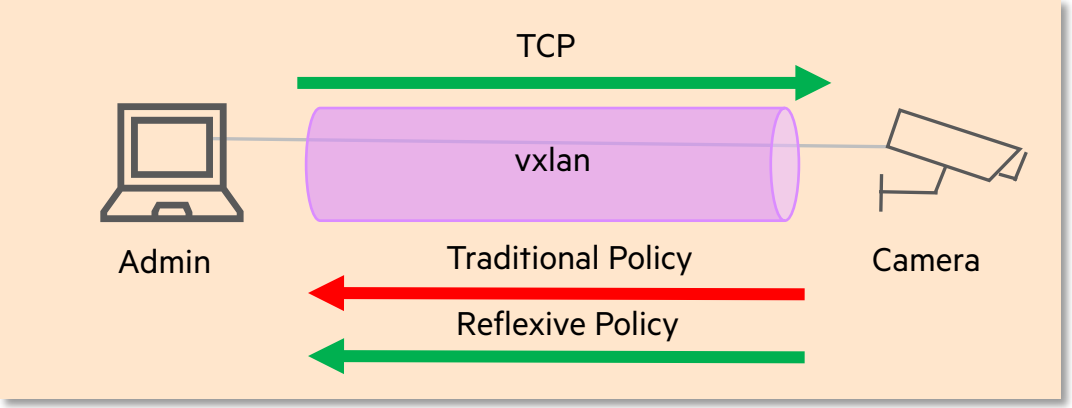


- Admin is permitted to access the TCP application on Camera.
- But all traffic from Camera to Admin should be blocked
- Traditional Policy - Blocks the return traffic that belongs to the same flow
- Reflexive Policy – Allow the return traffic if Admin initiated the application request.
- Note – If there is no match in the policy, traffic will be dropped by implicit deny all.

Micro & Macro Segmentation - GBP



Source	Destination	
	Admin	Camera
Admin	✓	✓
Camera	✗	✓




```
class gbp-ip Admin
    10 match tcp Camera Admin count
exit
port-access gbp Admin-GBP-Reflexive
    10 class gbp-ip Admin action reflect
exit
port-access role Admin
    associate gbp Admin-GBP-Reflexive
    vlan access 2
exit
```

Configuration

Configuration Task List - Reflexive PAP

1. Disabling IP Source Lockdown (Resource-Extended)
2. Flow Tracker Enablement
3. Reflexive PAP Creation — 10.13.0005
4. User Role Creation
5. GBP Role ID Assignment
6. Global enablement of Reflexive PAP — 10.13.0005
7. Global and Interface level enablement of port-access-security – 802.1x/Mac Auth

Configuration Task List – Reflexive GBP

1. VXLAN Infra Deployment – Static or EVPN
2. Disabling IP Source Lockdown (Resource-Extended)
3. Flow Tracker Enablement
4. Reflexive GBP Creation — 10.13.0005
5. User Role Creation
6. GBP Role ID Assignment
7. Global Enablement of GBP
8. Global enablement of Reflexive GBP — 10.13.0005
9. Global and Interface level enablement of port-access-security – 802.1x/Mac Auth

Global Enablement of Reflexive Policy – PAP and GBP

- To enable the use of reflexive PAP in the system

```
switch(config)#[no] port-access reflexive policy enable
```

- To enable the use of reflexive GBP in the system

```
switch(config)#[no] port-access reflexive gbp enable
```

- Above Configurations are Independent.

Reflexive PAP Creation

- To create a PAP with reflexive action -

```
switch(config)# port-access policy <policy-name>
switch(config-pa-policy)# class [ip|ipv6] <class-name> action
  cir              Specify the committed information rate
  drop             Drop all traffic
  dscp             Specify a Differentiated Services Code Point value
  ip-precedence    Specify the IP precedence
  local-priority   Specify a local priority value
  pcp              Specify the Priority Code Point (PCP) value
  redirect         Specify a redirect destination
  reflect          Allow traffic destined to a client only for flows initiated by client
  <cr>
```

```
switch(config)# port-access policy <policy-name>
switch(config-pa-policy)# class [ip/ipv6] <class-name> action reflect
switch(config-pa-policy)# exit
```

Reflexive GBP Creation

- To create a GBP with reflexive action -

```
switch(config)# port-access gbp <group-based-policy-name>
switch(config-pa-gbp)# class [gbp-ip|gbp-ipv6] <class-name> action
  drop     Drop all traffic
  reflect  Allow traffic destined to a client only for flows initiated by client
  <cr>
```

```
switch(config)# port-access gbp <group-based-policy-name>
switch(config-pa-policy)# class [gbp-ip|gbp-ipv6] <class-name> action reflect
switch(config-pa-policy)# exit
```

Reflexive PAP DUR Configuration

- To Configure the Reflexive PAP via DUR –

Configuration » Enforcement » Profiles » Edit Enforcement Profile - Reflexive-PAP

Enforcement Profiles - Reflexive-PAP

Summary | Profile | Attributes

	Type	Name		Value
1.	Radius:Aruba	Aruba-CPPM-Role	=	class ip tcp_sample_class 10 match tcp any 20.1.1.10 eq ssh count class ip udp_sample_class 10 match udp any 20.1.1.10 count port-access policy sample_reflexive_pap 10 class ip udp_sample_class 20 class ip tcp_sample_class action reflect port-access role windows associate policy sample_reflexive_pap vlan access 10

- Mandatory - Base role name GBP ID mapping should be configured via CLI in switch -

```
gbp role <base-role-name> <role-id>
```

REST – PAP

To Configure Policy Action Set for PAP -

POST /system/port_access_policies/{Port_Access_Policy.name}/cfg_entries/{Port_Access_Policy_Entry.sequence_number}/policy_action_set

Parameters

Cancel

Name	Description
Port_Access_Policy.name * required string *(path)*	Reference Resource: Port_Access_Policy Name of a port-access policy. Port_Access_Policy.name - Reference Resou
Port_Access_Policy_Entry.sequence_number * required string *(path)*	Reference Resource: Port_Access_Policy_Entry Policy entries as configured by the user. MAC based classes are not supported in a policy entry. The entire policy is rejected if it contains one or more policy entries with MAC classes. Port_Access_Policy_Entry.sequence_numbe

Request body

```
{
  "": "string",
  "cbs": 0,
  "cir": 0,
  "drop": true,
  "dscp": 0,
  "ecn": 0,
  "exceed_drop": true,
  "ip_precedence": 0,
  "local_priority": 0,
  "origin": "downloaded",
  "pcp": 0,
  "redirect": "captive-portal",
  "reflect": true
}
```

REST – PAP Contd..

To Create config entries for PAP -

POST /system/port_access_policies/{Port_Access_Policy.name}/cfg_entries

Parameters

Name	Description
Port_Access_Policy.name * required string *(path)*	Reference Resource: Port_Access_Policy Name of a port-access policy. Port_Access_Policy.name - Reference Resou


```
{
  "10": {
    "class": {
      "c1,ipv4": "/rest/v10.13/system/classes/c1,ipv4"
    },
    "comment": null,
    "origin": "local",
    "policy_action_set": "/rest/v10.13/system/port_access_policies/p1/cfg_entries/10/policy_action_set",
    "sequence_number": 10
  }
}
```

REST – GBP

To Configure Policy Action Set for GBP -

POST /system/port_access_gbps/{Port_Access_GBP.name}/cfg_entries/{Port_Access_GBP_Entry.sequence_number}/gbp_action_set

Parameters | Try it out

Name	Description
Port_Access_GBP.name * required string *(path)*	Reference Resource: Port_Access_GBP Port Access Group Based Policy name. Port_Access_GBP.name - Reference Resour
Port_Access_GBP_Entry.sequence_number * required string *(path)*	Reference Resource: Port_Access_GBP_Entry Policy entries as configured by the user. GBP policy entries must only be associated with GBP class entries. The policy is rejected if any associated classes that are of type other than GBP. Port_Access_GBP_Entry.sequence_number

Request body — application/json

Example Value | Schema

```
{
  "": "string",
  "drop": true,
  "origin": "local",
  "reflect": true
}
```

REST – GBP Contd..

To Create config entries for GBP -

POST /system/port_access_gbps/{Port_Access_GBP.name}/cfg_entries

Parameters

Try it out

Name	Description
Port_Access_GBP.name * required string *(path)*	Reference Resource: Port_Access_GBP Port Access Group Based Policy name. Port_Access_GBP.name - Reference Resour


```
{
  "10": {
    "class": {
      "class_icmp1,gbp-ipv4": "/rest/v10.13/system/classes/class_icmp1,gbp-ipv4"
    },
    "comment": null,
    "gbp_action_set": "/rest/v10.13/system/port_access_gbps/g1/cfg_entries/10/gbp_action_set",
    "origin": "local",
    "sequence_number": 10
  }
}
```

Configuration Task List Detailed – PAP

List of Configurations to be enabled before client onboarding -

Disabling IP Source Lockdown (Resource-Extended)

```
no ip source-lockdown resource-extended
```

Flow Tracker Enablement

Classifier Statement Creation

```
class [ip|ipv6] <class-name>
```

Reflexive PAP Creation

```
port-access policy <policy-name>
```

User Role Creation

```
port-access role <role-name>
    associate policy <policy-name>
exit
```

GBP Role ID Assignment

```
gbp role <role-name> <role-id>
```

Global enablement of Reflexive PAP

```
port-access reflexive policy enable
```

Global and interface level enablement of port-access-security – 802.1x/Mac Auth

```
interface <interface-id>
    no shutdown
```

Client Onboarding

```
Show port-access clients
```

```
port-access onboarding-method concurrent enable
aaa authentication port-access dot1x authenticator
    enable
aaa authentication port-access mac-auth
    enable
```

Configuration Task List Detailed – GBP

VXLAN Infra bring up – Static or EVPN

Disabling IP Source Lockdown (Resource-Extended)

Flow Tracker Enablement

GBP Classifier Statement Creation

GBP Creation & Association

```
no ip source-lockdown resource-extended
flow-tracker
class gbp-ip <class-name>
port-access gbp <policy-name>
    10 class gbp-ip <class-name> action reflect
exit
```

User Role Creation

Global enablement of Reflexive GBP

GBP Enable and Role ID assignment

```
Port-access role <role-name>
    associate gbp <policy-name>
exit
gbp enable
gbp role <role-name> <role-id>
```

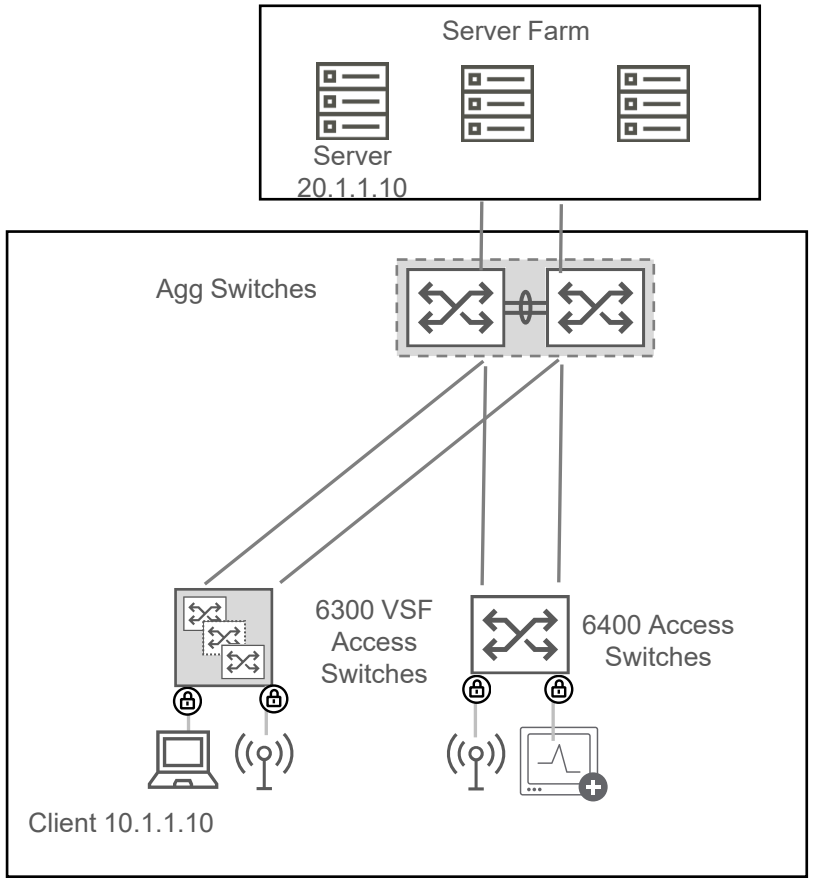
Global & interface level enablement of port-access-security – 802.1x/Mac Auth

Client Onboarding

```
    vlan access 1
    port-access onboarding-method concurrent enable
    aaa authentication port-access dot1x
authenticator
Show port-access clients
    enable
```

Demo

Reflexive PAP Demo



Client [10.1.1.10] <-> Server [20.1.1.10]

1. **ICMP - Non-Reflexive**
2. **SSH - Reflexive**

```
gbp role client 100
class ip sample_icmp
    10 match icmp any 20.1.1.10
class ip sample ssh
```

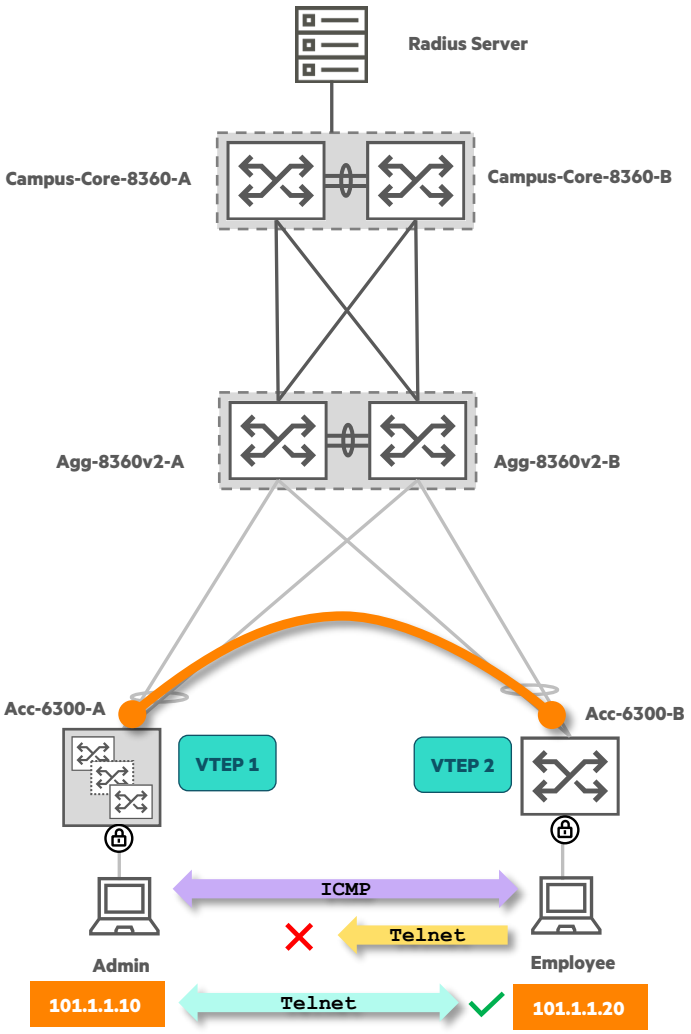
```
6300(config)# show resources

Resource Usage:

Mod  Description
         Resource                                      Used Reserved    Free
-----------------------------------------------------------------------------
---
1/1  Port Access Client Policy Lookup
         Ingress TCAM Entries                           18     2048
     Flex Lookup
         Ingress TCAM Entries                           20     2048
     Total
         Ingress TCAM Entries                           38     4096   16384
         Egress TCAM Entries                             0        0    8192
         Ingress Lookups                                 1                8
         Ingress Flex Lookups                            1                0
         Egress Lookups                                  0                4
         Ingress Policers                                0             2047
         Egress Policers                                 0             2047
2/1  Flex Lookup
         Ingress TCAM Entries                           16     2048
     Total
         Ingress TCAM Entries                           16     2048   18432
         Egress TCAM Entries                             0        0    8192
         Ingress Lookups                                 0                9
         Ingress Flex Lookups                            1                0
         Egress Lookups                                  0                4
         Ingress Policers                                0             2047
         Egress Policers                                 0             2047
```

```
    lag 1
exit
```

```
6300(config)# show ip flows
Source IP                    Dest IP                    Source  Dest    Proto  VRF     App   App          App
                                                        Port    Port                   ID    Name         Category
-----------------------------------------------------------------------------------------------------------------
10.1.1.10                    20.1.1.10                  53866   22      tcp    default 0
20.1.1.10                    10.1.1.10                  22      53866   tcp    default 0
```

```
6300(config)# show port-access clients detail
Port Access Client Status Details:
RADIUS overridden user roles are suffixed with '*'
Client 00:50:56:96:99:31
========================
  Session Details
  ---------------
    Port         : 1/1/1
    Session Time : 55s
    IPv4 Address :
    IPv6 Address :
    Device Type  :

  VLAN Details
  ------------
    VLAN Group Name :
    VLANs Assigned  : 10
      Access          : 10
      Native Untagged :
      Allowed Trunk   :

  Authentication Details
  ----------------------
    Status          : mac-auth Authenticated
    Auth Precedence : dot1x - Authenticating, mac-auth -
Authenticated
    Auth History    : mac-auth - Authenticated, 55s ago

Role Information:

Name  : client
Type  : local
-----------------------------------------------
    Access VLAN                          : 10
    Policy                               : sample_reflexive

Access Policy Details:
Policy Name   : sample_reflexive
Policy Type   : Local
Policy Status : Applied
Base Policy   : N/A
ACL Names     : N/A

SEQUENCE    CLASS                          TYPE ACTION
----------- ------------------------------ ---- ----------------
-----
10          sample_icmp                    ipv4 permit
20          sample_ssh                     ipv4 reflect

Class Details:
class ip sample_icmp
    10 match icmp any 20.1.1.10
class ip sample_ssh
    10 match tcp any 20.1.1.10 eq ssh
```

Reflexive GBP Demo




```
Access-VTEP-1(config)# show port-access clients detail

Port Access Client Status Details:

RADIUS overridden user roles are suffixed with '*'

Client 00:50:56:96:99:31
========================
  Session Details
  ---------------
    Port         : 1/1/1
    Session Time : 18s
    IPv4 Address :
    IPv6 Address :
    Device Type  :

  VLAN Details
  ------------
    VLAN Group Name :
    VLANs Assigned  : 101
      Access          : 101
      Native Untagged :
      Allowed Trunk   :

  Authentication Details
  ----------------------
    Status          : mac-auth Authenticated
    Auth Precedence : dot1x - Authenticating, mac-auth -
Authenticated
    Auth History    : mac-auth - Authenticated, 18s ago

  Authorization Details
  ---------------------
    Role   : Admin
    Status : Applied
```

```
    no shutdown
    no routing
    vlan access 1
    port-access onboarding-method concurrent enable
    aaa authentication port-access dot1x authenticator
        enable
    aaa authentication port-access mac-auth
        enable
```

Access VTEP 2

```
    gbp enable
    gbp role Admin 200
    gbp role Employee 201
    gbp role infra 2
    gbp role internet 3
    gbp role intranet 4
    class gbp-ip sample_icmp_allow
        10 match icmp Admin Employee
    class gbp-ip sample_tcp_allow
        10 match tcp Admin Employee
    class gbp-mac sample_arp_allow
        10 match Admin Employee arp
    vlan 1,3,101
    evpn
        vlan 101
            rd auto
            route-target export 4200000100:101
            route-target import 4200000100:101
    spanning-tree
    interface mgmt
        no shutdown
        ip dhcp
    port-access gbp sample_gbp_Employee
        10 class gbp-ip sample_icmp_allow
        20 class gbp-ip sample_tcp_allow
        30 class gbp-mac sample_arp_allow
    port-access role Employee
        associate gbp sample_gbp_Employee
        vlan access 101
    aaa authentication port-access dot1x authenticator
        enable
    aaa authentication port-access mac-auth
        addr-format multi-colon
        enable
    interface 1/1/2
        no shutdown
        no routing
        vlan access 1
        port-access onboarding-method concurrent enable
        aaa authentication port-access dot1x authenticator
            enable
        aaa authentication port-access mac-auth
            enable
```

Thank you

© 2023 Hewlett Packard Enterprise Development LP

Backup

Reflexive PAP - Sample Configuration

```
radius-server host <server-ip> key plaintext <key>
aaa group server radius <server-group>
    server <server-ip>
aaa authentication port-access dot1x authenticator
    radius server-group <server-group>
    enable
aaa authentication port-access mac-auth
    radius server-group <server-group>
    enable
no ip source-lockdown resource-extended
flow-tracking
              enable
exit
class [ip|ipv6] <class-name>
    10 match <protocol> <src> <dst> count
exit
port-access policy <policy-name>
       10 class [ip|ipv6] <class-name> action reflect
exit
port-access reflexive policy enable
port-access role <role-name>
    associate policy <policy-name>
exit
gbp role <role-name> <role-id>
interface <interface-id>
    no shutdown
    no routing
    vlan access 1
    port-access onboarding-method concurrent enable
    aaa authentication port-access dot1x authenticator
        enable
    aaa authentication port-access mac-auth
        enable
```

Note : ‘Count’ consumes hardware resource, hence its optional

Reflexive GBP - Sample Port Access Configuration

```
radius-server host <server-ip> key plaintext <key>
aaa group server radius <server-group>
    server <server-ip>
aaa authentication port-access dot1x authenticator
    radius server-group <server-group>
    enable
aaa authentication port-access mac-auth
    radius server-group <server-group>
    enable
no ip source-lockdown resource-extended
flow-tracking
              enable
exit
port-access reflexive gbp enable
class gbp-ip <class-name>
    10 match <protocol> <src-role> <dst-role> count
exit
port-access gbp <policy-name>
    10 class gbp-ip <class-name> action reflect
Exit
gbp enable
port-access role <role-name>
    associate gbp <policy-name>
exit
gbp role <role-name> <role-id>
interface <interface-id>
    no shutdown
    no routing
    vlan access 1
    port-access onboarding-method concurrent enable
    aaa authentication port-access dot1x authenticator
        enable
    aaa authentication port-access mac-auth
        enable
```