



**Hewlett Packard**  
Enterprise

User Guide

# **HPE Aruba Networking**

# **Identity-Based Traffic**

# **Management**

User Guide

# Important Notice

© Copyright 2024 Hewlett Packard Enterprise Development LP. The information contained herein is subject to change without notice. The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty.

Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein. Aruba Networks and the Aruba logo are registered trademarks of Aruba Networks, Inc. Third-party trademarks mentioned are the property of their respective owners. To view the end-user software agreement, go to [Aruba EULA](#).

Revision B, November 2024

Open Source Code:

Hewlett Packard Enterprise Company  
 Attn: General Counsel  
 WW Corporate Headquarters  
 1701 E Mossy Oaks Rd Spring, TX 77389  
 United States of America



## Contents

- ABOUT THIS GUIDE ..... 2
- 1 Aruba SD-WAN Identity-Based Traffic Management ..... 3
- 2 Prerequisites ..... 3
- 3 Identity-Based Traffic Management Overview ..... 3
- 4 Topology ..... 6
- 5 RADIUS Authentication Packet Exchanges ..... 6
  - 5.1 User-Profile Definition Setting ..... 7
  - 5.2 Customize the User-Profile Definition ..... 8
  - 5.3 View User-Profile Settings on the CLI ..... 8
  - 5.4 View User Identity Table on the CLI ..... 9
- 6 Identity-Based Traffic Management Policy Use Case Examples ..... 9
  - 6.1 Review of Zone-Based Segmentation ..... 9
  - 6.2 Identity-Based Segmentation ..... 10
  - 6.3 Proxy ARP and Private VLAN ..... 12
  - 6.4 Steering Traffic – Overlay ACL ..... 15



6.5 QoS Policy .....	16
6.6 Optimization (Boost) Policy .....	17
7 Monitoring .....	18
7.1 CLI .....	18
7.2 Other User-Profile CLI Commands .....	18
7.3 Identity Cache Persistence and Performance .....	18
7.4 View User Details in Orchestrator .....	19
Appendix A.....	21
Identify the ClearPass Service in Use for Authentication.....	21
Verify the Enforcement Policy .....	22
Verify Authentication Enforcement Profile .....	22

## **ABOUT THIS GUIDE**

The HPE Aruba Networking EdgeConnect Enterprise SD-WAN Platform enables customers to deploy identity-based traffic management to achieve optimal business outcomes from their Aruba SD-WAN infrastructure. This document serves as a technical introduction and provides insights regarding network design considerations and best practices for deployment. Field engineers and customer IT architects can use this document to assess the HPE Aruba Networking EdgeConnect Enterprise SD-WAN Platform, plan deployments, and exploit its business intent policies to deploy and manage robust, highly scalable SD-WAN infrastructure flexibly.

The audience for this document includes IT planners, network engineers, developers who will access the system, and SDWAN administrators. Please note that this document is not a training guide. It is assumed that the reader has, at minimum, foundational training in SD-WAN and ClearPass Essentials and, if possible, an Aruba Certified Professional (ACCP) certification.

The user of this guide should have a working knowledge of the following:

- AAA technologies (RADIUS, TACACS, 802.1X, MAC address authentication, and web authentication)
- Layer-2 and Layer-3 networking
- User identity stores, such as RADIUS, LDAP, and Active Directory For more details on the Aruba SD-

WAN platform, refer to the following:

- [Aruba ClearPass Policy Manager Documentation](#)
- [Aruba SD-WAN Product Documentation](#)



# 1 Aruba SD-WAN Identity-Based Traffic Management

HPE Aruba Networking is a pioneer in micro-segmentation, segmentation based on roles, user-based tunnels, VXLAN, and identity-based awareness. HPE Aruba Networking identity-based traffic management (IBTM) enables dynamically assigning SD-WAN traffic management policies based on identity match criteria such role-based access control (RBAC) username, user role, user group, user-mac address, device type, and identity context awareness from other sources. As soon as a person or device sends its first data packet, IBTM automatically applies traffic management policies that satisfy configurable identity criteria. For example, upon gaining access to the network, a user with the identity of a guest is automatically limited to accessing the internet and is denied access to all resources within the perimeter of that organization. Identity awareness is a cornerstone of HPE Aruba Networking's design philosophy across its product lines.

The following networking components are relevant for identity-based traffic management:

- **Orchestrator** provides central orchestration, management, and administration of EdgeConnect Gateways.
- **EdgeConnect** appliance gateways provide connectivity for edge devices.
- **ClearPass Policy Manager** (or any third-party RADIUS server that provides authentication and user identity information as part of the authentication process) provides role- and device-based secure network access control for IoT, BYOD, and corporate devices, as well as employees, contractors, and guests across any multivendor wired, wireless, and VPN infrastructure. IBTM is designed and tested with ClearPass Policy Manager (CPPM) in mind. EdgeConnect supports CPPM. CPPM can collect endpoint profile information from identity stores and different types of Aruba Instant Access Points (IAPs) and Remote Access Points (RAPs) via Aruba Activate.

## 2 Prerequisites

- HPE Aruba Networking SD-WAN Orchestrator, version 9.2 or later, with its policy match criteria configured to use RADIUS attributes.
- HPE Aruba Networking EdgeConnect SDWAN appliance software, version 9.2 or later.
- ClearPass Policy Manager with RADIUS server.



---

**NOTE:** Aruba supports ClearPass integration with Orchestrator, but other RADIUS servers work as well.

---

- A ClearPass Services Enforcement Policy (documented in [Appendix A](#)) must be configured. Enforcement policies specify what to match and which profile to execute.
- Endpoints such as PCs, mobile devices, and printers must be authenticating against a RADIUS server.
- Authenticator devices such as wireless access points or switches must have RADIUS authentication and accounting enabled.
- The RADIUS server must send appropriate return attributes, including user role information in RADIUS-Accept packets. For an example of how to configure a ClearPass server to return specific attributes, see [Appendix A](#).
- An EdgeConnect SDWAN appliance must be in the data path where RADIUS packets transit to the RADIUS server. Proxy ARP can force all site traffic to route through the EdgeConnect.
- EdgeConnect appliances listen on standard UDP 1812 and 1813 ports for RADIUS authentication and accounting exchanges. • RadSec (RFC6614) is not supported.

## 3 Identity-Based Traffic Management Overview

HPE Aruba Networking EdgeConnect appliances can automatically assign the right policies after a person or device authenticates to the network. EdgeConnect appliances support ClearPass out-of-the-box. The RADIUS roles assigned to users become the match criteria determining which policies the HPE Aruba Networking SD-WAN Orchestrator applies to that user's traffic, simplifying policy administration.

EdgeConnect uses multiple means to get user role information. User role, username, device type, user group, or user



MAC address match criteria are available to all policies, such as Overlay, Route Policies, Security Policies, QoS Policies, NAT, and so on. You can configure policies based on these match criteria for traffic steering, selecting firewall zones, or other policies.

The EdgeConnect gathers RADIUS role information from packets exchanged with the RADIUS server and populates its identity cache with the user ID, RADIUS role, IP address, MAC address of the device, and device type. RBAC role and device type become match criteria Orchestrator uses to determine which policies to use for managing traffic for firewalls, routing, traffic steering, QoS, Boost, and advanced security.

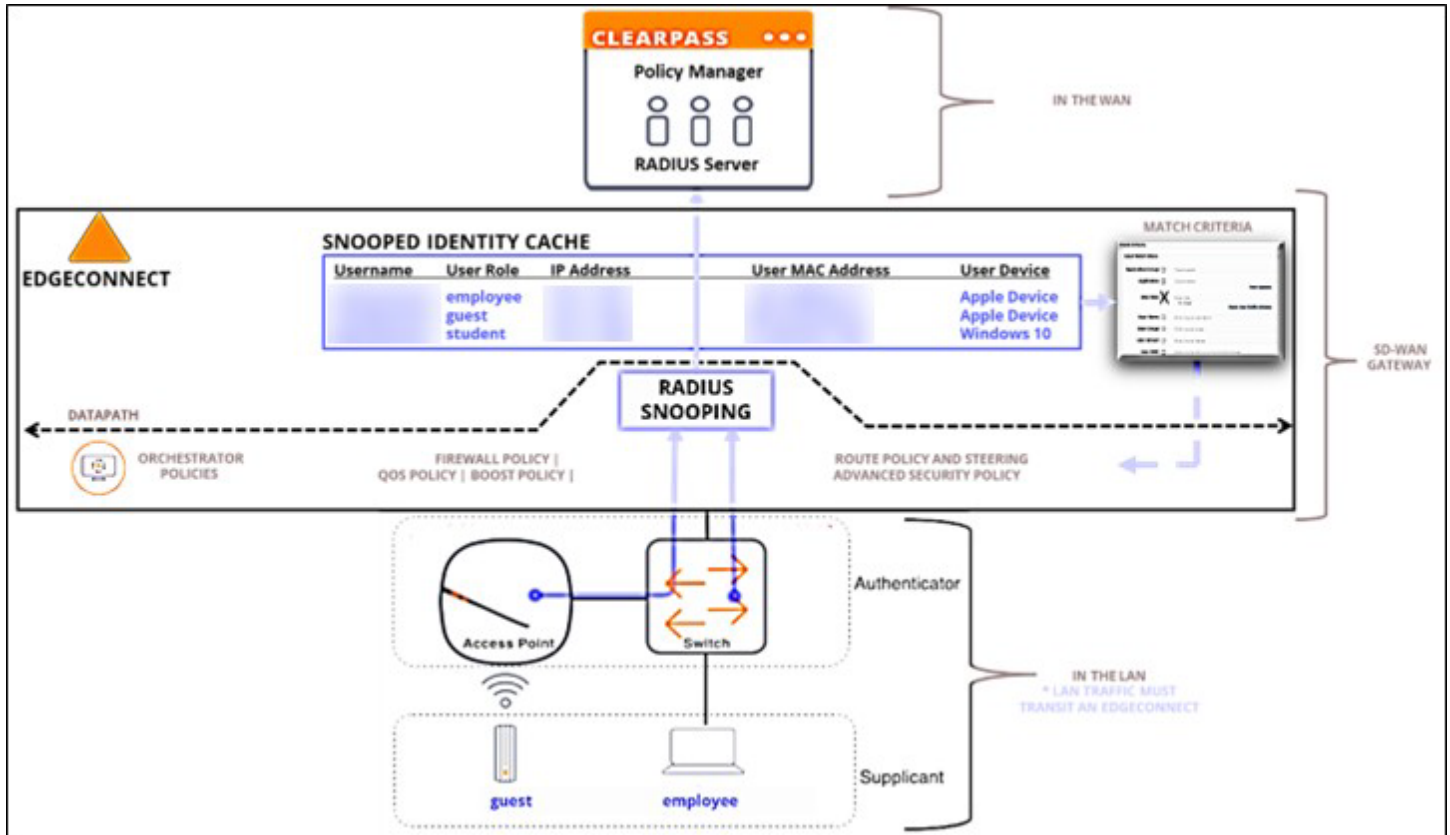


Figure 1. EdgeConnect Identity Cache.

For example, when two users connect to the network. One logs in as a guest via the wireless access point. This guest is assigned a policy that only allows internet access, and performance enhancement policies are not applied to guest traffic. The other user logs in as an employee via the switch. This employee is assigned a policy that gives full access to relevant internal systems, and performance enhancements are applied to the employee traffic. Orchestrator match criteria specify which policy is applied automatically.

For this feature to work in EdgeConnect, there is no requirement for a specific authentication method (such as dot1x, mac-auth, or captive-portal) or authentication protocol (such as PAP, MSCHAP-v2, or EAP-PEAP). EdgeConnect appliances inspect the RADIUS packet headers for specific information to build its identity table. The Orchestrator match criteria configuration options determine how policies are matched with RADIUS-authenticated flows. Configure match criteria in the Access Lists Template of the Orchestrator (navigate to **Configuration > Templates & Policies > Templates**, and then click **Access Lists** under Active Templates).

Attributes in RADIUS packets enable EdgeConnect appliances to cache the following user identity data:

- MAC address
- Framed IP address
- Username
- User device



- User role
- User group

RADIUS attributes become Orchestrator policy match criteria for traffic management policies that steer user or device traffic as soon as the network authentication is complete.

Identity-Based Traffic Management (IBTM) greatly simplifies SD-WAN operations. Policy administration is more automated and becomes much more straightforward.

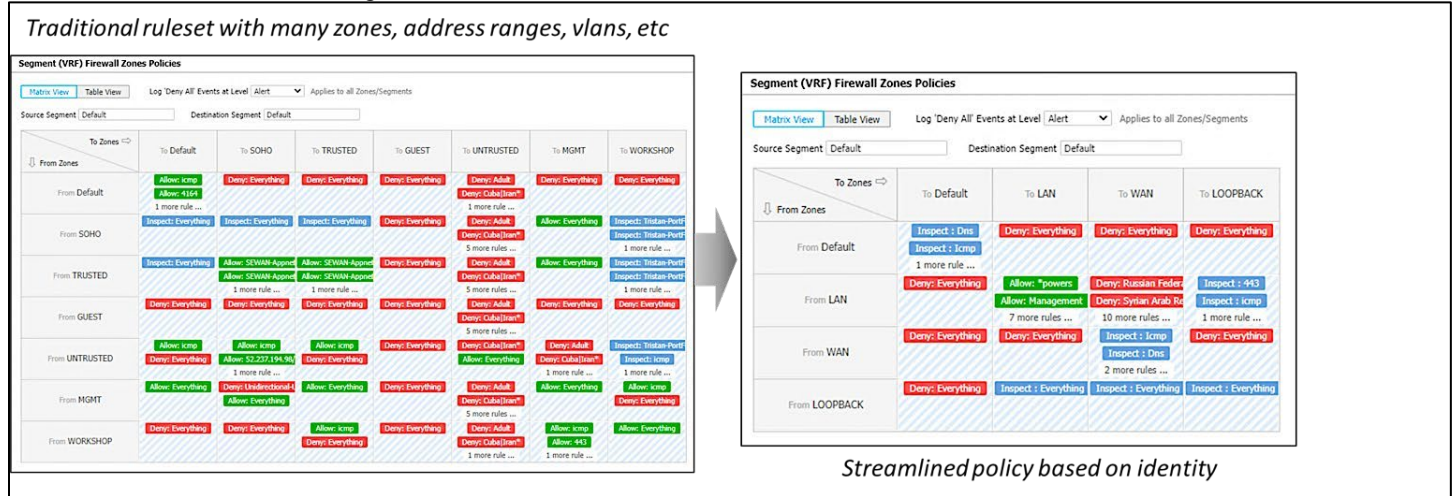


Figure 2. Simplified SD-WAN Operations.

IBTM can be applied as broadly or narrowly as required. The list below identifies some scenarios with obvious benefits:

- QoS Policy
  - For guest users, enable bandwidth on a “best effort” basis.
  - For a point-of-sale terminal, enable bandwidth on a real-time basis, perhaps using Boost.
- Traffic Steering
  - For IoT devices, deny access and do not send IoT traffic to Zscaler or Netskope.
  - For the Salesforce application, permit access and send to Netskope.
- Boost
  - For the NetFlow application, maximize network memory reduction and compress the IP header and payload.
  - For Either Address Group SEWAN-Appneta, compress the IP header and do not boost.
- Roles Within the Campus and Across the SD-WAN Fabric
  - For guest users, set low-priority QoS policy, disable IDS/IPS policy, and send direct internet access.
  - For employees, set high-priority QoS policy, enable IDS/IPS policy, and send internet access to Zscaler.
- Roles Within the Branch
  - For employee-to-guest, allow role-based access and use the firewall policy for Microsoft Teams. ○
  - For guest-to-employee, deny role-based access and use all firewall policies.



## 4 Topology

For RADIUS snooping to work, the following topology (Figure 3) is supported. In this topology, the authenticator (access point and switch) performs RADIUS authentication with authentication server (ClearPass) and the packets transit through the EdgeConnect appliance.

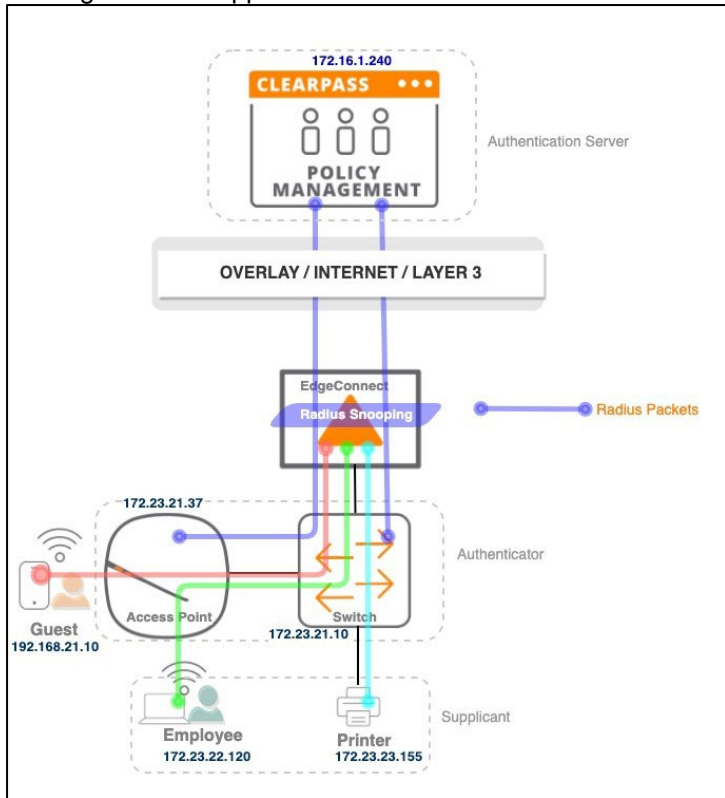


Figure 3. RADIUS Packets Flowing Through an EdgeConnect Appliance.



**NOTE:** The flow of the RADIUS packet must originate from the LAN side. EdgeConnect can only listen for RADIUS packets when the RADIUS authentication originates from the LAN (authenticator) toward the WAN side (RADIUS server is via overlay tunnel or internet) or the LAN (authenticator) to the LAN side (RADIUS server is in a local branch). If the RADIUS packet flow originates from the WAN side to the LAN side, then EdgeConnect does not listen for those packets.

## 5 RADIUS Authentication Packet Exchanges

An EdgeConnect appliance exchanges RADIUS authentication packets between the authenticator and the ClearPass RADIUS server. EdgeConnect appliances inspect RADIUS packet headers for certain information that build a user identity profile. Because the RadSec protocol encrypts the RADIUS packets, it cannot be used with HPE Aruba Networking identity-based traffic management.



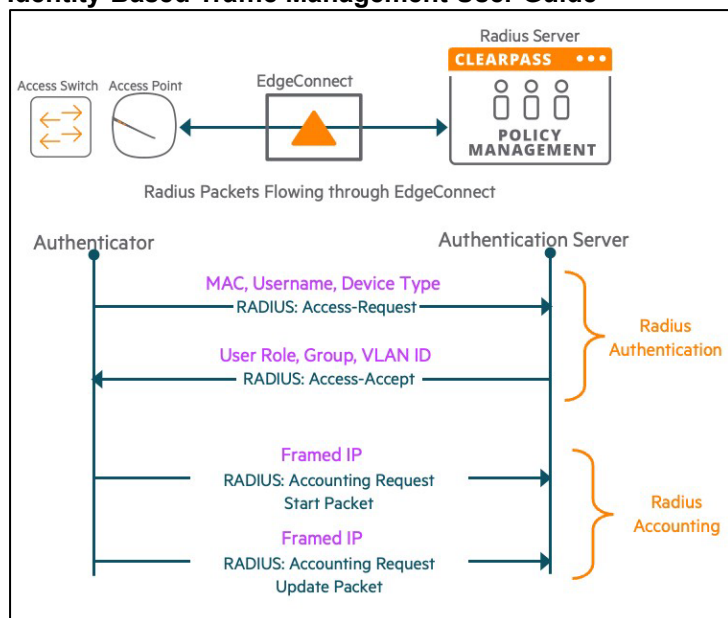


Figure 4. RADIUS Authentication Packet Exchanges Include Attributes That Populate the Appliance Identity Cache.

In the diagram above:

- Authentication requests include the username, device type, and MAC address.
- The RADIUS accept includes user role, group, and VLAN ID.



**NOTE:** A ClearPass enforcement policy and profile are required for the role to return a response.

- The client accounting request includes its framed IP address.
- ClearPass checks the accounting information and sends the Orchestrator the framed IP, user ID, and role.

RADIUS attributes are read by EdgeConnect appliances, including standard RADIUS attributes (defined in RFC2865) and vendor-specific attributes (VSAs). VSAs are unique to individual vendor implementations. For example, 14823 is the Aruba Vendor ID that defines attributes such as username, role, device, and VLAN.



**NOTE:** The MAC address and the framed IP address are key attributes for building the identity cache in the EdgeConnect. The identity cache cannot be built without these attributes present in the RADIUS packets.

## 5.1 User-Profile Definition Setting

A user-profile definition setting is predefined in the default definition file on the EdgeConnect appliance, which contains the following:

```
user-profile definition-file
"snooping|7|mac|ip|role|user|os|group|vlan,orch_attr|0,datatype|7|string|string|string|string|integer,display|7|User MAC|User IP|User Role|User Name|User Device|User Group|User Vlan,accounting-request|8:ip,access-request|1:user|31:mac|14823_12:os,access-accept|14823_10:group|14823_23:role|14823_1:role|14823_2:vlan"
```

This default definition file setting enables the EdgeConnect to look for the following standard attributes and Aruba VSAs from RADIUS packets to build the user identity table:

- MAC Address (Standard Attribute – IETF attribute ID:31) – Radius Request
- IP Address (Standard Attribute – IETF attribute ID:8) – Accounting Request
- Username (Standard Attribute – IETF attribute ID:1) – Radius Request
- User Role (Aruba Attribute – Aruba VSA ID:14823\_1 or 14823\_23) – Radius Accept

- User Group (Aruba Attribute – Aruba VSA ID:1482\_10) – Radius Accept
- User Device (Aruba Attribute – Aruba VSA ID:14823\_12) – Radius Request
- User Vlan (Aruba Attribute – Aruba VSA ID:14823\_2) – Radius Accept

In the ECOS 9.3.0.0 release and later, Orchestrator pushes this definition file through the Cloud Portal in a similar way to how other application definitions are pushed to the EdgeConnect.

## 5.2 Customize the User-Profile Definition

You can customize the user-profile definition setting for your requirements. For example, if you are using a third-party RADIUS server or a non-Aruba wired/wireless infrastructure that does not use Aruba VSA attributes, then you need to determine which RADIUS attribute ID corresponds to the attributes defined in the user-profile definition setting.

1. If you are already using Aruba-User-Role attributes in your HPE Aruba Networking wired or wireless LAN infrastructure with a third-party RADIUS server (for example, Free RADIUS, Cisco ISE, or Microsoft NPS), then no further changes are required to the user-profile definition setting, as it is likely the RADIUS attribute is already configured in your RADIUS server return attributes.

If RADIUS packets are transiting through the EdgeConnect gateway, RADIUS attributes will be snooped and the user identity table built.

If you do not have the Aruba-User-Role provisioned in your RADIUS server return attribute, then you must make that change on your RADIUS server. This ensures that the RADIUS server sends the Aruba-User-Role attribute as part of the RADIUS accept packet.

2. If you are using a third-party wired or wireless infrastructure to authenticate endpoints, then you must identify your vendor's equivalent of user role. For example, Cisco WLC may use `Aire-ACL-Name` as its equivalent. In this case, the user role attribute ID would be `14179_6`. You can append this attribute ID in the user-profile definition settings. Similarly, the `group`, `vlan`, and `os` attributes can also be appended to match your vendor-specific attribute.

Consider this example of a `user-profile definition-file` command for a Cisco Aire-ACL-Name as user role:

**config t**

```
user-profile definition-file
"snooping|7|mac|ip|role|user|os|group|vlan,orch_attr|0,datatype|7|string|string|string|str
ing|string|string|integer,display|7|User MAC|User IP|User Role|User Name|User Device|User
Group|User Vlan,accounting-
request|8:ip,accessrequest|1:user|31:mac|14823_12:os|14179_XX:os,access-
accept|14823_10:group|14179_XX:group|14823_23:role|14823_1:role|14179_6:role|14179_XX:rol
e|14823_2:vlan|14179_XX:vlan"
```

**XX** → Corresponds to respective vendor's radius attribute ID

As in the above example, do not delete anything on the existing user-profile definition setting, and always append to the existing settings.



**NOTE:** There is no separate command for appending a configuration. You must use the whole command, as shown above, and add your specific attributes at the end of your respective identity attribute. It is a single command:

```
user-profile definition-file "<the whole definition in one single line with comma
separated value>"
```

## 5.3 View User-Profile Settings on the CLI



**NOTE:** This is applicable only to ECOS 9.4.1.0 or later.



To view the user-profile definition settings, log in to the EdgeConnect Gateway CLI either via SSH or through Orchestrator by right-clicking the appliance in the appliance tree and then clicking **CLI Session**. Then, issue the `tunbug gu7` command to view the current user-profile definition setting:

```
DASLAB-EntraBranch # tunbug gu7
snooping|7|mac|ip|role|user|os|group|vlan
orch_attr|0
datatype|7|string|string|string|string|string|integer
display|7|User MAC|User IP|User Role|User Name|User Device|User Group|User Vlan
accounting-request|8:ip
access-request|1:user|31:mac|14823_12:os
access-accept|14823_10:group|14823_23:role|14823_1:role|14823_2:vlan
DASLAB-EntraBranch #
```

Figure 5. View User-Profile Settings on the CLI.

## 5.4 View User Identity Table on the CLI

To view the user identity table, log in to the EdgeConnect Gateway CLI either via SSH or through Orchestrator by right-clicking the appliance in the appliance tree and then clicking **CLI Session**. Then, issue `tunbug gu4` command to view the currently cached user identity table:

```
DASLAB-RackN9-S-1 # tunbug gu4
Mac Address|IP Address|User Name|User Device|User Role|User Group|
-----
00188BD8F5FF|0|172.23.22.56|unknown|unknown|unknown|unknown
204c034a58e3|0|172.23.22.156|cape-guest|NOFP|guest|BYOD
e4b318dc17de|0|172.23.22.153|printer-101|Win 10|printer|BYOD
047D7B07768B|0|172.23.22.57|unknown|unknown|unknown|unknown
000d60778a3e|0|172.23.22.55|printer-101|Win 7|printer|BYOD
74de2b68bd1b|0|172.23.22.151|lab-guest|Win 7|guest|BYOD
```

Figure 6. View User Identity Table on the CLI.

# 6 Identity-Based Traffic Management Policy Use Case Examples

You can create identity-based traffic management (IBTM) policies in Orchestrator. Several typical examples are described in the subsections that follow.

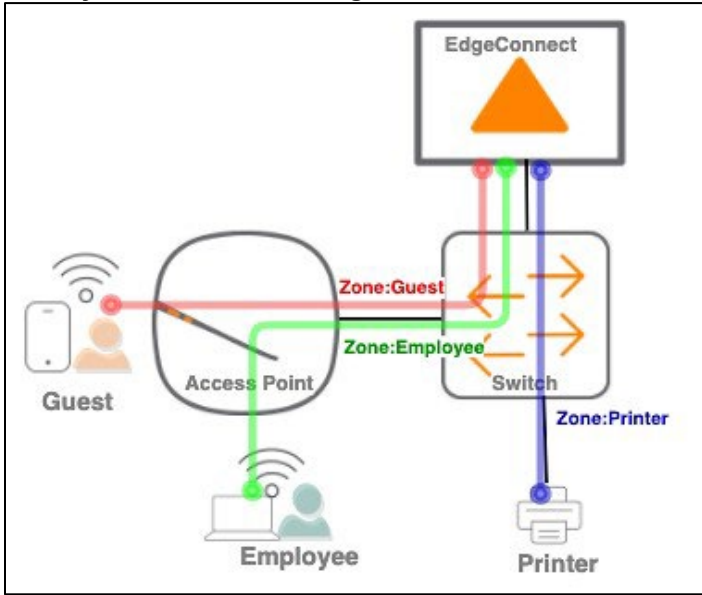
## 6.1 Review of Zone-Based Segmentation

Without an identity-based segmentation, networks are placed in various zones, with zone-based firewall policies built to restrict traffic between zones. Creating zones and zone-based firewalls can get complex quickly if you must manage numerous zones and policies between them. But with identity-based segmentation, zones and security policies between them can be simplified greatly.

Here, zone-based segmentation is illustrated with a simple example of users and devices with a role of Guest and the specification that these users and devices should not be allowed to print. Meanwhile, users or devices with a role of Employee should be allowed to print and access the corporate network.

Figure 7 shows typical zone-based segmentation, where networks and subnets are placed on respective zones and firewall policies are built around the zone to permit or deny traffic between them and allow desired traffic only. In this example, Guest zone users and devices are allowed to browse the internet only via the Default zone, and are denied reaching Printer or Employee zones completely.





Security Policy (Zone Based Segmentation)			
From Zone	To Zone	Match Criteria	Action
Guest	Printer	Match Anything	Deny
Guest	Default	Port 80,443,123,53,67,68	Permit
Guest	Employee	Match Anything	Deny
Guest	Default	Match Anything	Deny
Employee	Printer	Match Anything	Permit
Employee	Default	Match Anything	Permit
Default	Default	Match Anything	Permit

Figure 7. Zone-Based Segmentation Topology.

## 6.2 Identity-Based Segmentation

The RADIUS snooping feature on EdgeConnect can extend the identity-based security policy from the LAN to the WAN edge. Enabling RADIUS snooping simplifies the zone-based configuration using user identity data, reducing the need to create many zones and manage complex security policies between them.

In the example below (Figure 8), identity-based segmentation is illustrated with the same example as section 6.1. Here, all users and devices are authenticated by network devices (switches and access points) against an authentication server using the RADIUS protocol. Assuming that all users and devices are fully authenticated, the authentication server sends the `Aruba-User-Role` attribute part of the RADIUS authentication (or the equivalent attribute corresponding to a user role), and the switch or access point sends the `Framed-IP-Address` attribute part of the RADIUS accounting, then EdgeConnect can build user-identity profile mapping the username, role, and MAC address to the respective IP address.



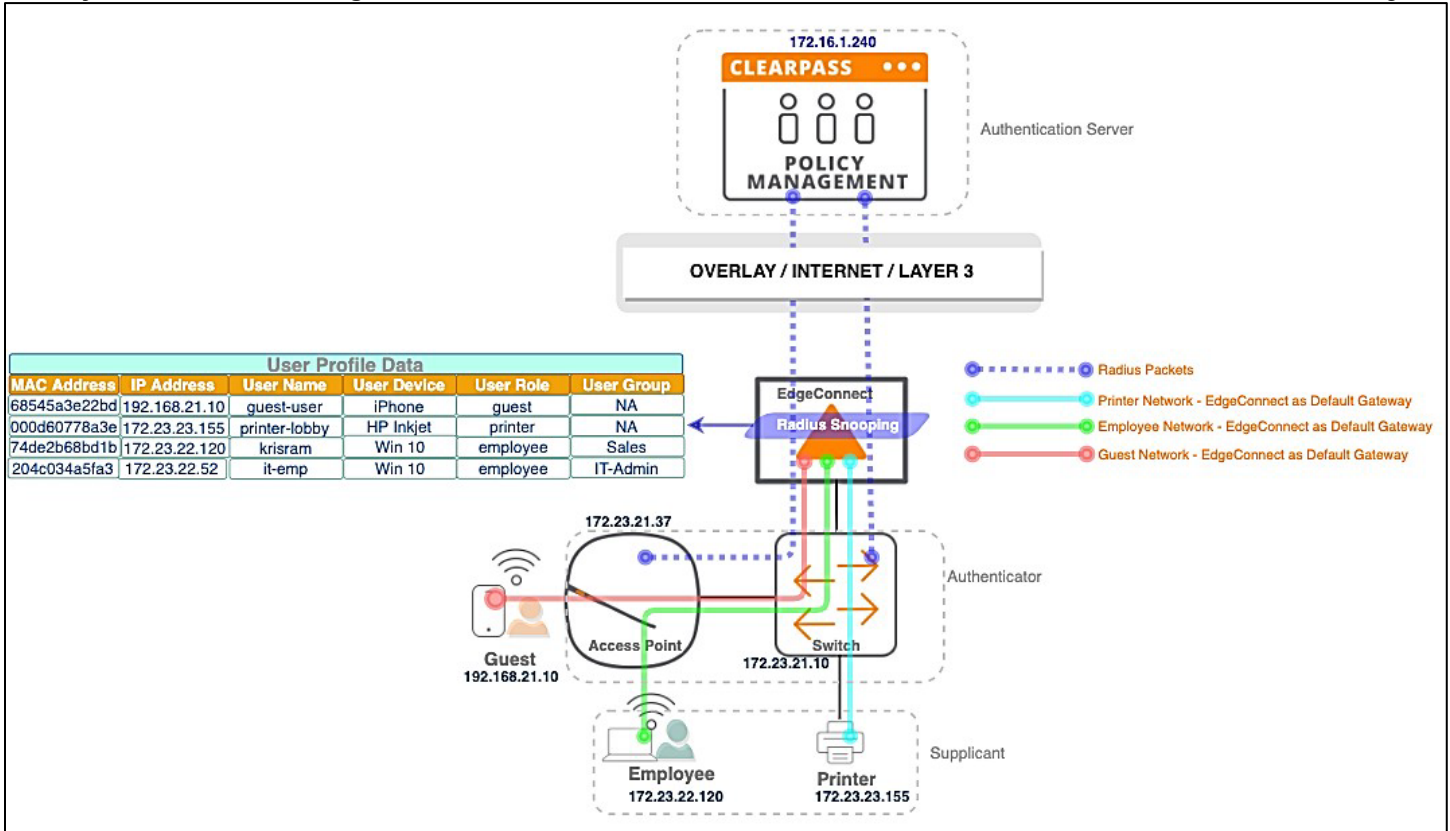


Figure 8. Identity-Based Segmentation Topology.

Now, the zone-based firewall policy can be simplified by placing Guest, Employee, and Printer in the same Zone (for example, UNTRUSTED) and configuring firewall policies using the user identity (username, role, or user group).

Figure 9 shows the simplified firewall policy where all networks are considered under UNTRUSTED zone and segmented policies are defined to restrict traffic based on the user role identity.

Security Policy (Identity Based Segmentation)			
From Zone	To Zone	Match Criteria	Action
UNTRUSTED	UNTRUSTED	Source Role: guest, Dest Role: printer	Deny
UNTRUSTED	UNTRUSTED	Source Role: employee, Dest Role: printer	Permit
UNTRUSTED	UNTRUSTED	Port 80,443,123,53,67,68, User Role: guest	Permit
UNTRUSTED	UNTRUSTED	User Role: guest	Deny
UNTRUSTED	UNTRUSTED	Everything	Permit

Figure 9. Identity Based Segmentation – Firewall Policy.

Figure 10 shows the actual configuration represented on Orchestrator between zone-based segmentation and identitybased segmentation.



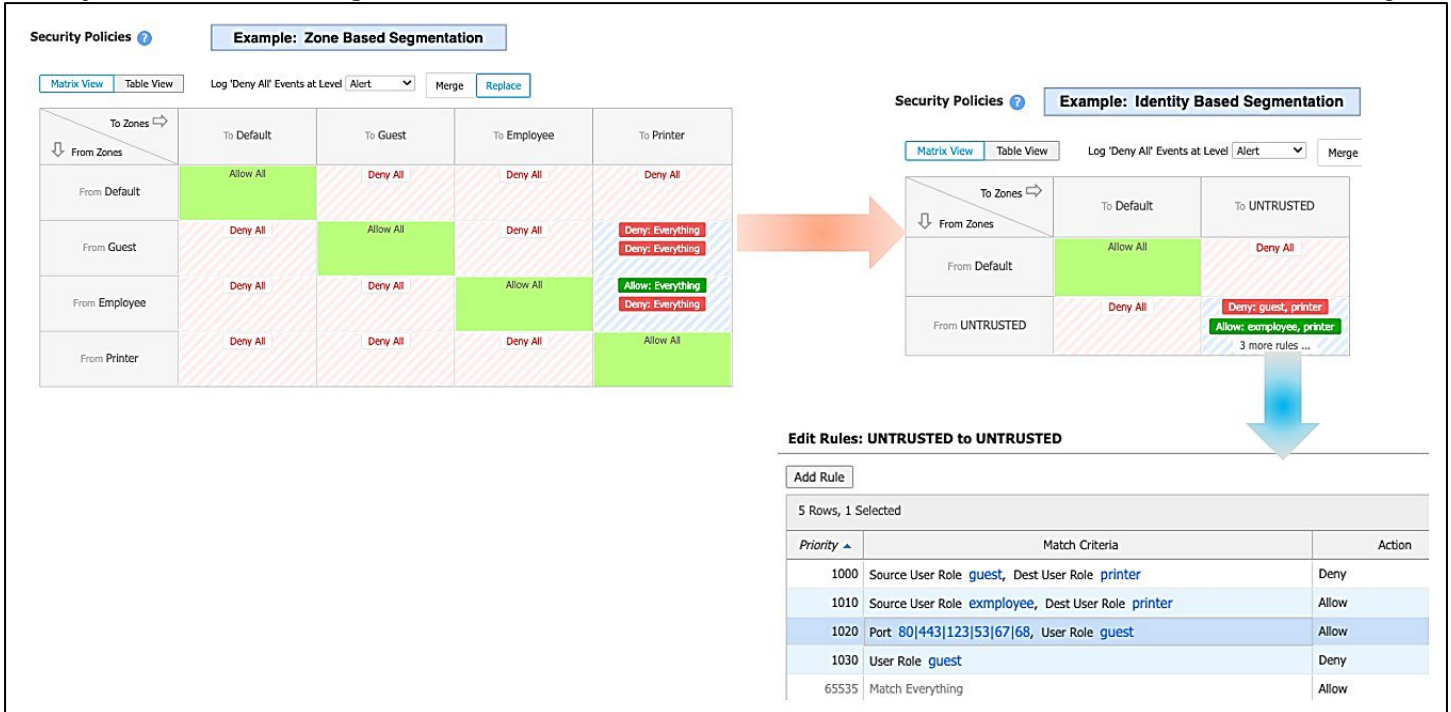


Figure 10. Simplified Configuration View on HPE Aruba Networking SD-WAN Orchestrator.

### 6.3 Proxy ARP and Private VLAN

Fundamental to enforcing identity-based policy between subnets or user roles within the EdgeConnect (also known as “East-West policy enforcement”) is properly directing traffic to the EdgeConnect gateway. If user traffic is switched or routed locally before it touches the EdgeConnect, then policy cannot be enforced.

The private VLAN feature on switches (where the user or access point is connected) is key to ensuring that all VLAN traffic is forced to the EdgeConnect gateway. When user traffic hits the EdgeConnect, security policies can be applied based on identity. Proxy ARP must be enabled on the EdgeConnect on LAN/VLAN interfaces where policy enforcement is required.



**NOTE:** The use of Proxy ARP and private VLAN is required only when you want to enforce policy for users or endpoints within or between VLANs. Enable Proxy ARP only on LAN interfaces where you want to enforce identity-based firewall policy.

By using private VLAN on switches and enabling the proxy-arp setting on EdgeConnect, all Layer-3 traffic between endpoints becomes subject to security policy based on user identity.

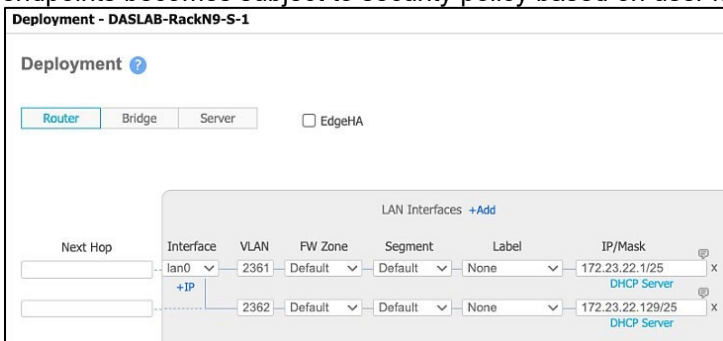


Figure 11. Private VLAN Feature on the Deployment Tab.

In this example, lan0.2361 and lan0.2362 are the two interfaces where user traffic is subject to security policy:



```
DASLAB-RackN9-S-1 # config t DASLAB-RackN9-S-1
(config) # proxy-arp ?
<interface or label name>
DASLAB-RackN9-S-1 (config) # proxy-arp lan0.2361
DASLAB-RackN9-S-1 (config) # proxy-arp lan0.2362
```

To check the status of Proxy ARP on the interfaces:

```
DASLAB-RackN9-S-1 (config) # show proxy-arp lan0.2361
interface name  proxy-arp status -----
---  ----- lan0.2361
Enabled
DASLAB-RackN9-S-1 (config) # show proxy-arp lan0.2362
interface name  proxy-arp status -
-----
lan0.2362          Enabled
```

Here is a private VLAN sample configuration on an HPE Aruba 3810 (AOS-S) switch:

```
EdgeConnect-LAN-Switch2# show run vlan 2363 !
vlan 2363 → Primary VLAN
private-vlan primary    private-vlan
isolated 63
    tagged 1-2,13-48 → tag the ports that connected to the EdgeConnect or uplink switch
ip address 172.23.24.10 255.255.255.128    ip source-interface radius vlan !
vlan 63 → Private VLAN
    untagged 3-12 → untag the Ports to which PC/printers or other endpoints connected
no ip address !
```

Here is a Private VLAN sample configuration on an HPE Aruba 6300 (AOS-CX) switch:

```
vlan 2363 → Configure Primary VLAN
private-vlan primary !
vlan 63 → Configure Secondary/Isolated VLAN
private-vlan isolated primary-vlan 2363 !
interface 1/1/1 → Ensure uplink port to the EdgeConnect is allowing primary VLAN and
port-type as Promiscuous    no shutdown    no routing    vlan trunk native 1
vlan trunk allowed 1,2363    private-vlan port-type promiscuous    exit !
interface 1/1/6 → Configure the ports where endpoints connected with isolated VLAN and
port-type as secondary    no shutdown    no routing    vlan access 63
    private-vlan port-type secondary
exit !
```

To verify the private VLAN and port status:

```
show private-vlan port-type -----
Port      Port-type
-----
1/1/1     promiscuous
1/1/6     secondary
1/1/7     secondary
1/1/8     secondary
1/1/9     secondary
1/1/10    secondary
1/1/11    secondary
1/1/12    secondary
show private-
vlan
----- Primary
Isolated      Community
```



2319	19	-
2320	20	-
2363	63	-



### 6.4 Steering Traffic – Overlay ACL

Identity-based policies can be configured using the user identity on the match Overlay ACL match criteria, such as username, MAC address, or user role.

Figure 12 illustrates an example of using user identity in an Overlay ACL to redirect all Employee internet-bound traffic (HTTP/HTTPS) to the CASB overlay.

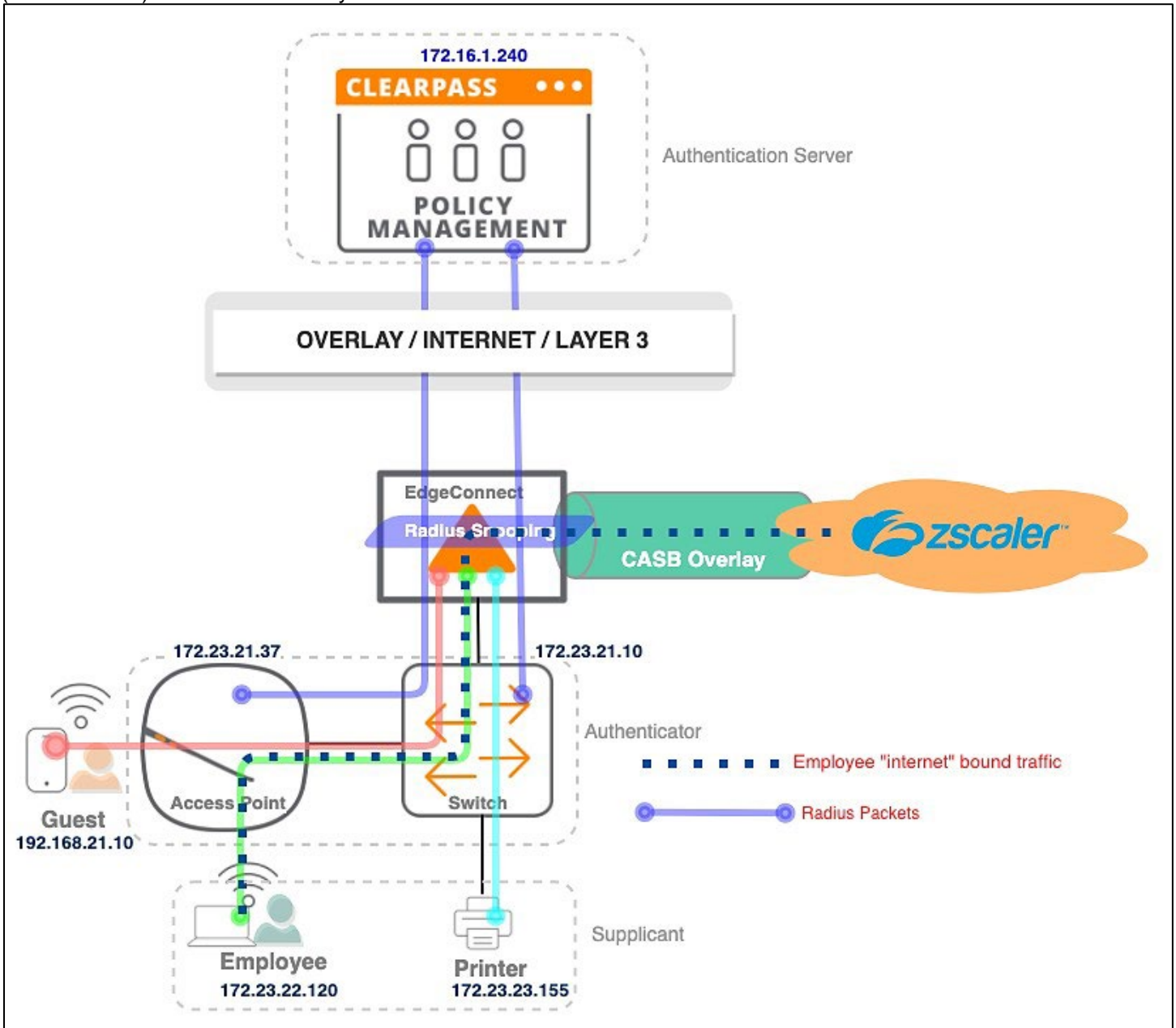


Figure 12. Steering Traffic to a Specific Overlay.

Policy can be written as follows (Figure 13) on the Business Intent Overlay (BIO) page of a given overlay to select only traffic flows matching a specific user role or user group in that overlay. This example shows the BIO configuration page, where modifying the Overlay ACL policy makes any host matching the user role **Employee** or user group **Corp or Sales or Marketing or Research** AND **Internet** traffic (port 80 or 443) subject to the CASB Overlay and breaks out internet traffic to Zscaler Cloud.



**Business Intent Overlays**

Priority	Overlay	Region	Topology	Primary Interfaces	Backup Interfaces	QoS & Security	Policy Order	Primary Interfaces	Backup Interfaces
1	RealTime Match Traffic Overlay ACL	Global Regions ▶	Regional Mesh	INET1 INET2 INET3 MPLS1 MPLS2 LAB1		High Availability Waterfall: Overall Quality	1 Break out 2 Backhaul	INET1 INET2	LTE
2	<b>CASB</b> Match Traffic Overlay ACL	Global Regions ▶	Regional Mesh	INET1 INET2 INET3 MPLS1 MPLS2 LAB1		High Efficiency Balanced: Link Utilizatio...	1 Zscaler Cloud 2 Break out 3 Backhaul	INET1 INET2	LTE

**Overlay Configuration**

Name: CASB    Match: Overlay ACL    Protocol: tcp, Port: 80|443, User Role: employ...

**Associate ACL**

Priority	Match Criteria	Permit	
1060	Protocol tcp, Port 80 443, Fabric/Internet Internet, User Role employee	permit	✗
1070	Protocol tcp, Port 80 443, Fabric/Internet Internet, User Group Corp Sales Marketing Research	permit	✗

Figure 13. Business Intent Overlay Page to Configure Identity-Based Overlay Policy.

### 6.5 QoS Policy

Using user-profile attributes, QoS (Quality of Service) policies can be written to provide a differentiated quality of experience based on device type, user role, or other user attributes.

For example, suppose you want to use user identity in a QoS policy to apply different traffic class and LAN/WAN QoS to streaming device, guest, and management traffic. In Figure 14, QoS policy is defined to apply varying levels of traffic class and DSCP marking based on the identity of the user or device.

**QoS Policies**

DASLAB    Active Map    Add Map    Delete Map    Rename Map    DSCP Marking Override

Add Rule    Merge    **Replace**    All rules on the appliance will be DELETED and replaced.

Priority	Match Criteria	Traffic Class	LAN QoS	WAN QoS
1000	User Device Fire TV   Apple TV   Roku TV   Chromecast	7 - Streaming	af41	af41
1010	User Role management	5 - Management	ef	ef
1020	User Role guest	6 - Guest	be	be
1030	Match Everything	1 - RealTime	trust-lan	trust-lan

Figure 14. QoS Policy Configuration Using User Identity.



Here, streaming devices are put in the **Streaming** traffic class with LAN-side and WAN-side QoS marked to **AF41**. Flows with the user role **Management** are treated differently, with QoS set to **EF** and shaper policy to **Management**.

### 6.6 Optimization (Boost) Policy

Applying identity-based attributes when building optimization policy can be useful to preserve Boost bandwidth for more useful applications and provide improved quality of experience for high-demand applications.

Figure 15 below illustrates an example of how to use user identity in optimization policy to enable network memory/TCP accel for the Employee user role, or any username beginning with “emp.” The configuration shows the optimization policy where a combination of username, user role, and user group provides disparate Boost usage based on user identity.

**Optimization Policies** ?

DASLAB-Boost ▾  Active Map

All rules on the appliance will be DELETED and replaced.

5 Rows, 1 Selected

Priority ▲	Match Criteria	Network Memory	IP Header Compression	Payload Compression	TCP Accel	TCP Accel Details	Protocol Accel
1010	User Role <a href="#">guest</a>   <a href="#">IoT gaming</a>	disabled	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<a href="#">i</a>	none
1020	User Role <a href="#">employee</a> , User Group <a href="#">Storage</a>	minimize latency	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<a href="#">i</a>	none
1040	User Name <a href="#">*emp</a>	balanced	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<a href="#">i</a>	none
1045	Application <a href="#">Cfs_smb</a> , Either IP/Subnet <a href="#">172.16.23.0/24</a>	balanced	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<a href="#">i</a>	none
1050	Match Everything <a href="#">↗</a>	minimize latency	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<a href="#">i</a>	none

Figure 15. Optimization Policy Using User Identity.



## 7 Monitoring

You can monitor identity-based traffic management information using ClearPass Policy Manager (CPPM), HPE Arube Networking SD-WAN Orchestrator, and the command line interface (CLI).

### 7.1 CLI

Tunbug provides the following identity cache details:

- **tunbug gu4** provides the entire identity cache.

Select an EdgeConnect appliance and open a CLI session for that appliance. To view the user table, run `tunbug gu4`:

```
DASLAB-RackN4-US-1 #
DASLAB-RackN4-US-1 # tunbug gu4
Mac Address|IP Address|User Name|User Device|User Role|User Group|
-----|-----|-----|-----|-----|-----|
204c034a58e3|0|172.23.21.33|cape-guest|NOFP|guest|BYOD
DASLAB-RackN4-US-1 #
DASLAB-RackN4-US-1 #
```

Figure 16. Tunbug gu4 Display of an Appliance Identity Cache.



**NOTE:** Identity cache entries expire and delete if the user is idle—in other words, if there are no active flows from a given client—for one hour. Also, the user expires immediately upon receiving the `accounting-stop` RADIUS packet for a given client.

- **tunbug gu3** provides specific entry details, including IP address and segment information:

```
Enter a Valid Client Ip address: 10.26.159.20
Enter Segment: Default
WARNING: terminal is not fully functional
User Profile for IP:10.26.159.20 (press RETURN)
```

```
-----
- mac: 204c0338b24d user:
arubauix os: OS X role: sp_hr
VLAN: unknown group: unknown
Context State: Active
No .of Flows using this ctx :0 → Only if this number is 0 do we remove the user
entry.
```

### 7.2 Other User-Profile CLI Commands

- **user-profile RADIUS snooping <enable/disable>** enables or disables RADIUS snooping.
- **user-profile delete all** deletes all information entered by the user. This delete action does not reset any active flows. New flows are subject to the user identity table or policy at the time of flow creation.
- **user-profile delete ip <ip-address> segment <segment-name>** deletes a specific user entry based on IP and VRF segment. This delete action does not reset any active flows for that IP address. New flows are subject to the user identity table or policy at the time of flow creation.

### 7.3 Identity Cache Persistence and Performance

In the current release of ECOS software, user identity cache is saved on a per-appliance basis. Identity cache is not an orchestrated function that is typical to EdgeConnect operation. Even if there are two EdgeConnects operating in an HA pair at a single site, they do not share this identity cache between them. This behavior will be enhanced in future releases to synchronize user identity cache between appliances in an HA pair.

Identity cache entries are expired and deleted in the following scenarios:



- The user is idle—in other words, there are no active flows from a given client—for one hour.
- The user is expired immediately upon receiving an accounting-stop RADIUS packet for a given client.

Identity cache contents are saved to disk and restored upon reboot. EdgeConnect restores the older cache that is less than 10 minutes old. If the cache is more than 10 minutes old, then it is not restored.

HPE Aruba SD-WAN appliances gather RADIUS attributes at the rates below:

- Each appliance maintains up to 64,000 user entries, independent of hardware models.
- RADIUS snooping rate is gathered at the rate of new flow creation supported by the system.

### 7.4 View User Details in Orchestrator

You can also view user information for flows in the Orchestrator UI.

1. Navigate to the Flows tab (**Monitoring > Bandwidth > Flows > Active & Recent flows**).
2. Right-click any column header to display a list of column options.
3. When viewing active flows, include at least **User Name**, **Source Role**, **Dest Role**, and **User Device**.

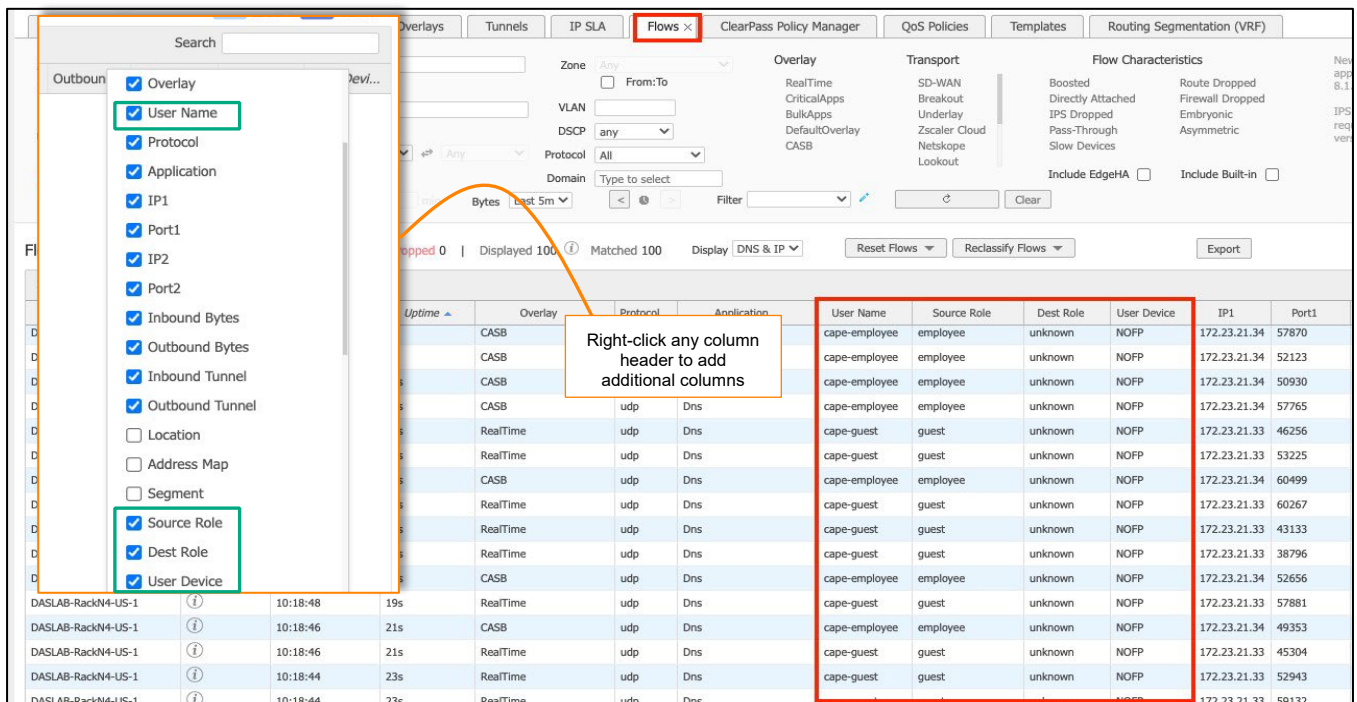


Figure 17. Add Additional Columns on the Flows Tab.

4. To view additional information for a flow, click the Information (i) icon in the Detail column of a given flow.
5. Click the User Details tab to view Source and Destination user details based on the identity cache built by the RADIUS snooping feature.





**NOTE:** This detail is only available when the corresponding IP and user role are already available in the identity table.

**Flow details for IP1: 172.23.26.57 Port1: 0 IP2: 172.23.26.60 and Port2: 0**

General Optimization TCP NAT AVC/DNS Internet Performance **User Details** Flow Decision Identity

Source User Details		Destination User Details	
User MAC	204c034a5fa3	User MAC	204c034a58e3
User Role	employee	User Role	guest
User Name	cape-employee	User Name	cape-guest
User Device	NOFP	User Device	NOFP
User Group	BYOD	User Group	BYOD
User Vlan	6	User Vlan	6
Derived User Role	employee	Derived User Role	guest

Figure 18. Flow Details Showing Source/Destination User Details When Available.



# Appendix A

EdgeConnect gateways rely on RADIUS packet header information to build identity cache. One important aspect of mapping the user role to an IP address is returning the proper RADIUS attribute from the RADIUS server.

This section details an example of how an HPE Aruba ClearPass RADIUS server (CPPM) is configured to return the Aruba-User-Role (VSA ID: 14823\_1) attribute as part of the authentication process. Here, you can see a CPPM configuration relate to authentication policy (Services) and post-authentication RADIUS attributes returned that are part of the enforcement policy and profile.

## Identify the ClearPass Service in Use for Authentication

In your environment, you must identify which service policy is used for wired or wireless authentication so you can verify that the service enforcement policy is configured to send proper return attributes.

There are several ClearPass services configured in the screenshot below. In your own CPPM UI, navigate to **Configuration > Services**, and then click the service that need to be modified. The example below looks at the **DASLAB1X-CPPM** service to view the enforcement policy in use.

The screenshot displays the 'Configuration > Services' page in the ClearPass UI. The left pane shows a table of services, with 'DASLAB-1X-CPPM' highlighted. The right pane shows the configuration for 'DASLAB-1X-CPPM', including authentication methods, sources, and enforcement policy. An arrow points from the highlighted service in the list to the 'Enforcement Policy' field in the configuration pane, which is set to 'RK - Radius Policy'.

#	Order	Name	Type	Template
1.	1	[AirGroup Authorization Service]	RADIUS	RADIUS Enforcement ( Generic )
2.	2	DASLAB-1X-CPPM	RADIUS	Aruba 802.1X Wireless
3.	3	DASLAB-CP-CPPM	RADIUS	RADIUS Enforcement ( Generic )
4.	4	RK_AOS-CX_DOT1X-Authentication	RADIUS	RADIUS Enforcement ( Generic )
5.	5	PDM-SSH-LOGIN-CP	RADIUS	802.1X Wired
6.	6	RK-Home-Wireless-Mac-Auth	RADIUS	MAC Authentication
7.	7	SD-WAN-VPN-1AP Auth	RADIUS	MAC Authentication
8.	8	Anshul-C2C	RADIUS	Aruba 802.1X Wireless
9.	9	C2C-dot1X Wireless	RADIUS	802.1X Wired
10.	10	C2C-AP55-incorrectchannel	RADIUS	Aruba 802.1X Wireless
11.	11	AOSCX-Switch-MAC	RADIUS	MAC Authentication
12.	12	VIA1X Aruba VPN Authentication	RADIUS	RADIUS Enforcement ( Generic )
13.	13	VIA Aruba VPN Authentication		
14.	14	Split-Tunnel		
15.	15	UBT-LUR-Anshul		
16.	16	UBT-DUR-Anshul		
17.	17	DAS-VIA-Users		
18.	18	[Aruba Device Access Service]		
19.	19	802.1X WIRED		
20.	20	[Policy Manager Admin Network Login Service]		

Configuration > Services > Edit - DASLAB-1X-CPPM

**Services - DASLAB-1X-CPPM**

Summary Service Authentication Roles Enforcement

**Service:**

Name: DASLAB-1X-CPPM  
 Description: Aruba 802.1X Wireless Access Service  
 Type: Aruba 802.1X Wireless  
 Status: Enabled  
 Monitor Mode: Disabled  
 More Options: -

Match ALL of the following conditions:

Type	Name
1. Radius:IETF	NAS-Port-Type
2. Radius:IETF	NAS-Identifier

**Authentication:**

Authentication Methods: 1. [EAP PEAP]  
 2. [EAP\_MSCHAPv2]  
 3. [PAP]  
 4. [MSCHAP]

Authentication Sources: 1. ERT-2008-Server [Active Directory]  
 2. [Local User Repository] [Local SQL DB]

Strip Username Rules: -  
 Service Certificate: -

**Roles:**

Role Mapping Policy: -

**Enforcement:**

Use Cached Results: Disabled  
 Enforcement Policy: RK - Radius Policy

Figure 19. Identify the CPPM Service in Use for Authentication.

After identifying the service and enforcement policy in use, you can view the enforcement policy to see which enforcement profile is being used to return attributes post-authentication.

1. In the CPPM UI, navigate to **Configuration > Enforcement > Policies** to look for your existing enforcement policy. In this example, **RK – Radius Policy** has been identified as the enforcement policy in use.
2. After selecting one of the conditions listed in the policy, click **Edit Rule**.

Configuration » Enforcement » Policies » Edit - RK - Radius Policy

Enforcement Policies - RK - Radius Policy

Summary Enforcement **Rules**

Rules Evaluation Algorithm:  Select first match  Select all matches

Enforcement Policy Rules:

Conditions	Actions
1. (Date:Day-of-Week BELONGS_TO Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, Sunday)	RK_Aruba-User-Role, RK_EC_Post to Orchestrator - Profile
2. (Date:Day-of-Week BELONGS_TO Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, Sunday)	DC1-OrchHA_Post to Orchestrator - Profile

Add Rule Copy Rule Move Up ↑ Move Down ↓ **Edit Rule** Remove Rule

Figure 20. RADIUS Enforcement Policy.

The Rules Editor appears.

3. Look under the Enforcement Profiles header to view enforcement profiles in use.

Rules Editor

Conditions

Match ALL of the following conditions:

Type	Name	Operator
1. Date	Day-of-Week	BELONGS_TO
2. Click to add...		

Enforcement Profiles

Profile Names:

- [RADIUS] RK\_Aruba-User-Role
- [Post Authentication] RK\_EC\_Post to Orchestrator - Profile

Move Up ↑ Move Down ↓ Remove

Figure 21. View Enforcement Profiles.



**NOTE:** Contact your CPPM administrator if you are unsure about which policy to modify, or which enforcement policy is used for user and device authentication.

## Verify Authentication Enforcement Profile



An enforcement profile is mapped to an enforcement policy to ensure that certain attributes are returned to the authenticator part of the RADIUS-accept packet.

The example below illustrates the enforcement profile returning `Aruba-User-Role` or other equivalent attributes for a given vendor.



**IMPORTANT:** Enforcement profile and return attributes vary depending on how CPPM policy has been designed in your environment. To find out what specific attribute can be configured, contact your CPPM administrator.

To view authentication enforcement profiles in the CPPM UI, navigate to **Configuration > Profiles**, and then click the enforcement profile that is attached to the enforcement policy.

Configuration » Enforcement » Profiles » Edit Enforcement Profile - RK\_Aruba-User-Role

Enforcement Profiles - RK\_Aruba-User-Role

Summary		Profile		Attributes	
Type	Name	Value			
1. Radius:Aruba	Aruba-User-Role	=	%{Authorization:[Local User Repository]:Role_Name}	Returns	Aruba-User-Role attribute derived from Local user
2. Radius:Hewlett-Packard-Enterprise	HPE-User-Role	=	%{Authorization:[Local User Repository]:Role_Name}	Returns	HPE-User-Role attribute derived from Local user
3. Radius:Aruba	Aruba-User-Role	=	%{Authorization:ERT-2008-Server:memberOf}	Returns	Aruba-User-Role attribute derived from Active Directory Group Member
4. Radius:Airespace	Airespace-ACL-Name	=	%{Authorization:ERT-2008-Server:memberOf}	Returns	Cisco-ACL-Name attribute derived from Active Directory Group Member
5. Radius:IETF	Filter-Id	=	%{Authorization:ERT-2008-Server:memberOf}	Returns	Filter-ID standard attribute derived from Active Directory Group Member
6. Radius:Airespace	Airespace-ACL-Name	=	%{Authorization:[Local User Repository]:Role_Name}	Returns	Filter-ID standard attribute derived from Local user database

Figure 22. Click the Enforcement Profile Attached to the Enforcement Policy.

