

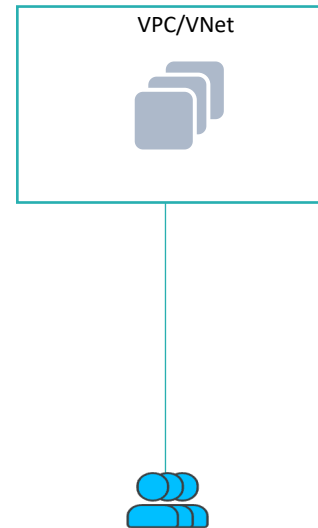


User VPN

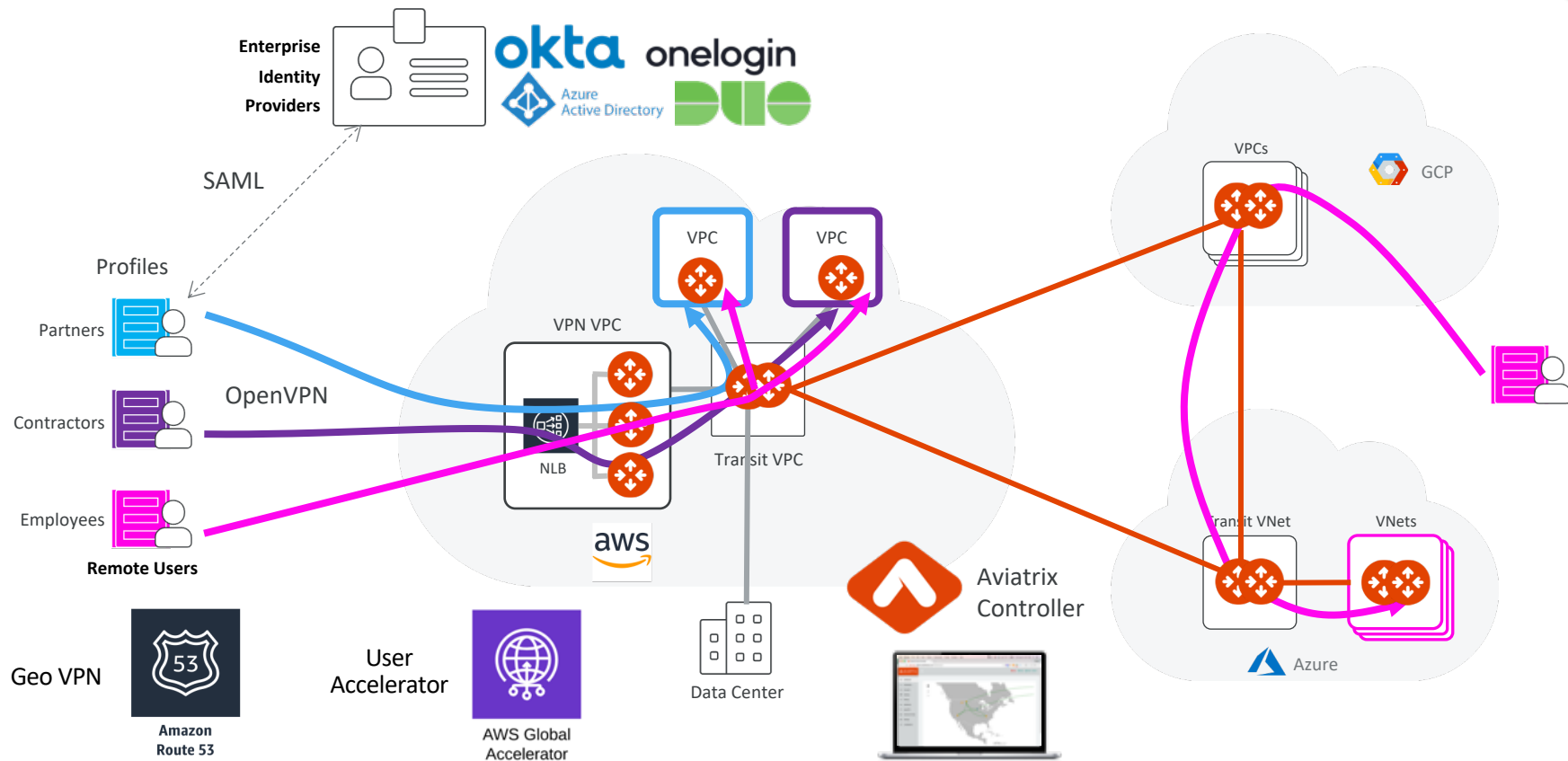
ACE Solutions Architecture Team

Problem Statement

- Connect **users** securely and seamlessly to public cloud resources
- **Least latency** accessing the cloud resources
- Cloud-native: **should not backhaul** to on-premises Data Center first
- Enterprise-grade: **Identity Provider** integration
- **Multicloud** repeatability



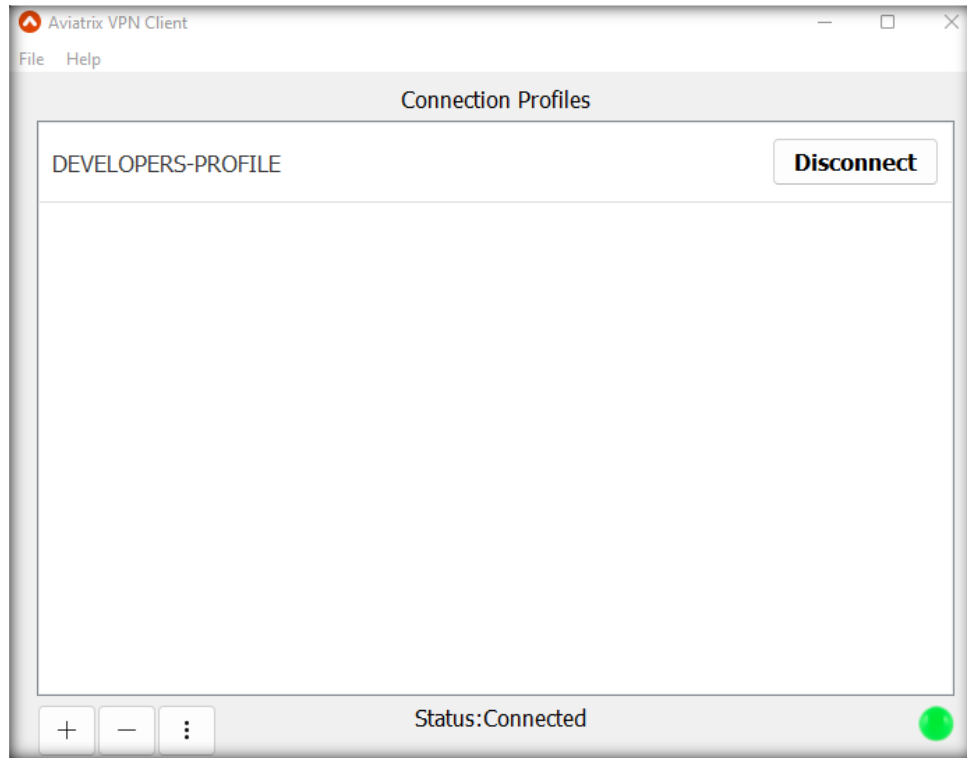
User VPN Overview



Client Software



- OpenVPN Client
 - All OpenVPN client software are supported. The supported clients are macOS, Windows iOS, Android, Chromebook, Linux and BSD
- Aviatrix VPN Client
 - Aviatrix VPN Client supports macOS, Windows, Linux Debian distribution, and BSD distribution
 - Choose Aviatrix VPN Client if you require SAML authentication directly from VPN client software



<https://docs.aviatrix.com/previous/documentation/latest/aviatrix-openvpn/download-vpn-client.html>

Automated Load Balancer



- The controller automatically launches a cloud-native load balancer based on the cloud type
- Automates target groups to attach Aviatrix VPN gateways to the LB
- The domain name of the cloud provider's load balancer, such as AWS ELB, will be the connection when a VPN user connects to the VPN gateway
- Seamless relaunch of VPN Gateways after deletion without reissuing a new .ovpn cert file

Create Load Balancer Actions

Filter by tags and attributes or search by keyword

Name	DNS name	State	VPC ID
Aviatrix-vpc-00ff16450xd34a...	Aviatrix-vpc-00ff16450xd34a...	active	vpc-00ff16457ad2174ff

Load balancer: Aviatrix-vpc-00ff16450xd34ab56

Filter by tags and attributes or search by keyword

Name	Port	Protocol	Target type	Load Balancer	VPC ID
Aviatrix-vpc-00ff16450xd34a...	943	TCP	instance	Aviatrix-vpc...	vpc-0...

Target group: Aviatrix-vpc-00ff16450xd34ab56

Description Targets Health checks Monitoring Tags

The load balancer starts routing requests to a newly registered target as soon as the registration process completes and the demand increases, you can register additional targets. If demand on your targets decreases, you can deregister targets.

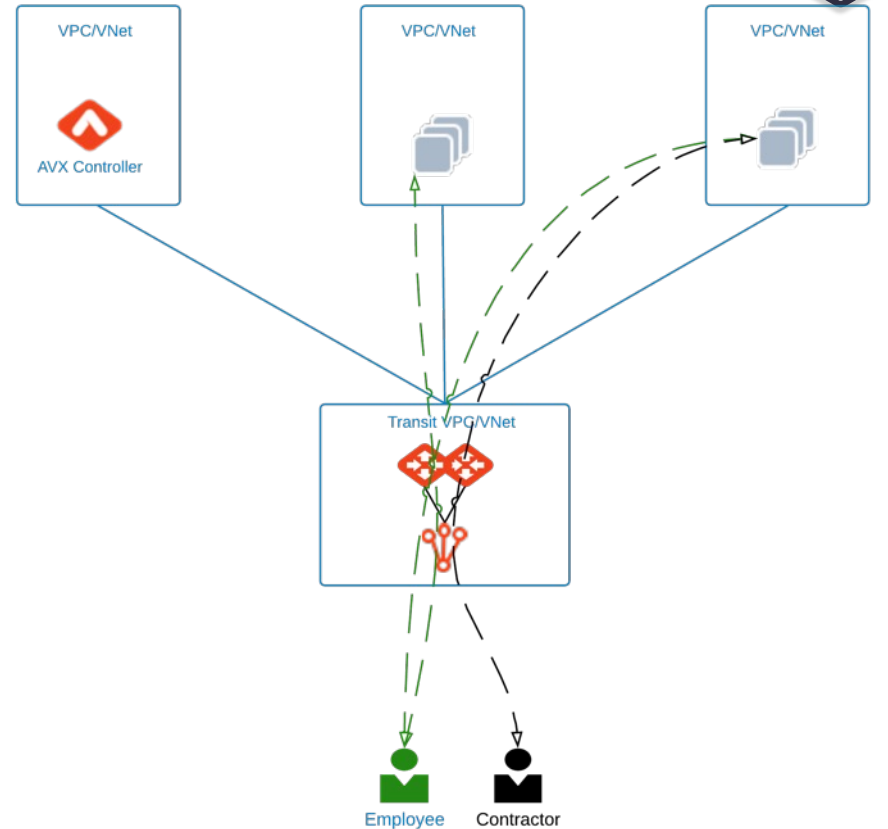
Edit

Registered targets

Instance ID	Name	Port	Availability Zone	Status
i-0552e63461a12a9a7	aviatrix-AWS-UW2-SAML-VPN-GW-1	943	us-west-2a	healthy
i-0beab155cd99db9ff	aviatrix-AWS-UW2-SAML-VPN-GW-2	943	us-west-2b	healthy

Profile-Based Security Policies

- A user is dynamically assigned a virtual IP address when connected to a gateway
- Isolation between employees, contractors, partners, or developers
- Supports multiple profiles
- Automated firewall rules
- Security based on user not source IP
- The security policy is dynamically pushed to the landing Aviatrix VPN gateway when a VPN user connects
- It is only active when a VPN user is connected
- When a VPN user disconnects, the security policy is deleted from the VPN gateway



Secure Assertion Markup Language

- Supports IDPs like Azure AD, Okta, Duo, Office 365
- User accounts are onboarded on the IDP portal
- Users can be onboarded on Aviatrix controller if SAML is not required

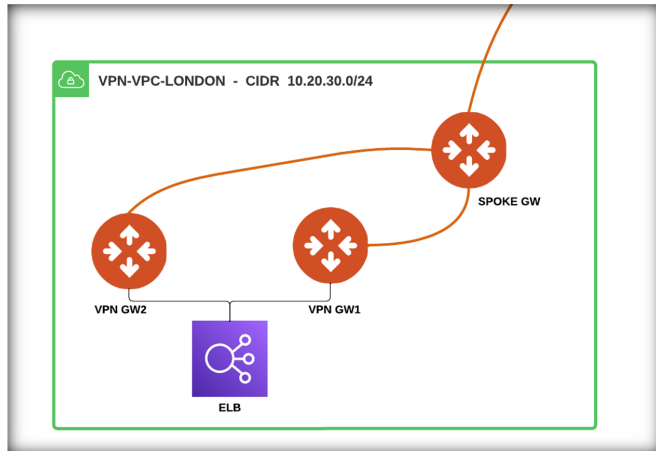


AWS SSO



Ad-hoc VPN VPC

- Create a dedicated VPC
 - Select the **Default** VPC (i.e. Spoke VPC)
- This VPC will host both the VPN Gateways, the ELB and the Spoke Gateways



Create VPC/VNet

Name: VPN-VPC-LONDON

Cloud: **aws** Standard

Account: aws-account

Region: eu-west-2 (London)

VPC CIDR: 10.20.30.0/24

VPC Function: **Default**

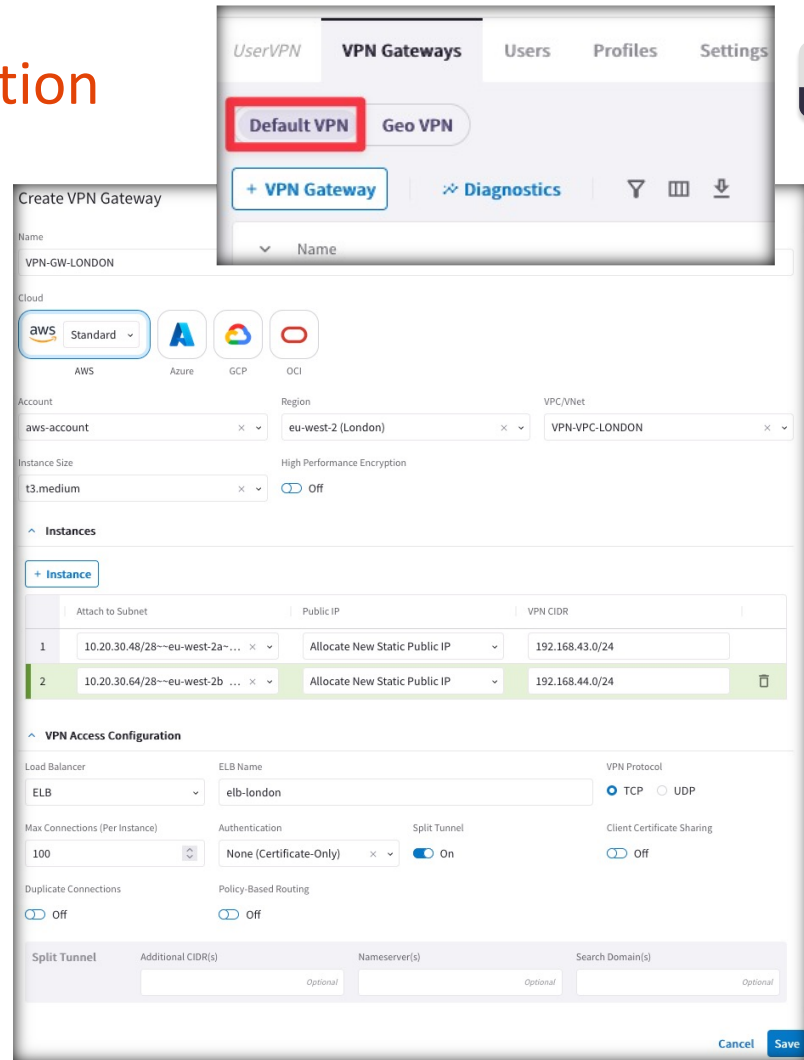
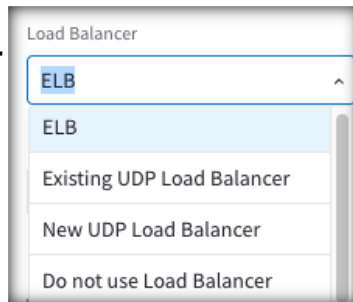
Advanced Settings

Cancel Save

The screenshot shows the 'Create VPC/VNet' form with various fields. A red arrow points to the 'Default' option in the 'VPC Function' dropdown menu.

Default VPN Gateways and ELB Creation

- Configure one or more VPN Gateways
 - Each VPN Gateway must be configured with its own **VPN CIDR Block**
 - When a VPN user connects to the VPN gateway, the user will be assigned a virtual IP address from the VPN CIDR Block
 - The default IP address pool is **192.168.43.0/24**
- The ELB template is pre-configured by default
 - Depending on the cloud type you selected, you can select:
 - **ELB**
 - **Existing UDP Load Balancer**
 - **New UDP Load Balancer**
 - **No Load Balancer**



Geo VPN Gateways and ELB Creation

- Configure one or more VPN Gateways
 - Each VPN Gateway must be configured with its own **VPN CIDR Block**
 - When a VPN user connects to the VPN gateway, the user will be assigned a virtual IP address from the VPN CIDR Block
 - The default IP address pool is **192.168.43.0/24**
- The ELB template is pre-configured by default
- Geo VPN configuration options:
 - Domain Name: this domain name must be hosted by AWS Route53
 - VPN Service: the hostname that users will connect to

The screenshot displays the AWS Management Console interface for creating a Geo VPN Gateway. The top navigation bar includes tabs for 'UserVPN', 'VPN Gateways', 'Users', 'Profiles', and 'Settings'. The 'VPN Gateways' tab is active, and the 'Geo VPN' sub-tab is selected. The main content area shows the 'Create Geo VPN Gateway' wizard. The 'Cloud' section is set to 'AWS'. The 'Account' is 'aws-account', 'Region' is 'eu-west-2 (London)', and 'VPC/Net' is 'VPN-VPC-LONDON'. The 'Instance Size' is 't3.medium' and 'High Performance Encryption' is 'Off'. The 'Instances' section shows two instances, each with a public IP address of 192.168.43.0/24. The 'VPN Access Configuration' section shows 'Load Balancer' set to 'ELB', 'ELB Name' set to 'ELB-LONDON', 'VPN Protocol' set to 'TCP', 'Max Connections (Per Instance)' set to '100', 'Authentication' set to 'None (Certificate-Only)', 'Split Tunnel' set to 'On', and 'Client Certificate Sharing' set to 'Off'. The 'Split Tunnel' section shows 'Additional CIDR(s)', 'Nameserver(s)', and 'Search Domain(s)' fields. The 'Geo VPN Configuration' section shows 'Account' set to 'aws-account', 'Domain Name' set to 'vpngw.route53london.com', and 'Service Name' set to '193.13.32.45'. The 'Save' button is highlighted in blue.

Create the Spoke GW inside the VPN VPC

- After the VPN Gateways deployment:
 - Create the Spoke Gateway inside the VPN VPC
 - The AviaTriX Controller will take care of the routing between the VPN Gateway and the Spoke Gateway
 - Attach the Spoke Gateway to any Transit Gateways such that the VPN Gateway will be able to be interconnected to the MCNA

Create Spoke Gateway

Name

SPOKE-GW-LONDON

Cloud

aws Standard

AWS

Azure

GCP

OCI

Alibaba

Account

aws-account

Region

eu-west-2 (London)

VPC/VNet

VPN-VPC-LONDON

Instance Size

t3.micro

High Performance Encryption

Off

Attach To Transit Gateway

AVX-AWS-TRANSIT-GW

Advanced Settings

BGP

Off

Instances

+ Instance

Attach to Subnet

Public IP

1

10.20.30.48/28~eu-west-2a~VPN-VPC-LONDON-Publi...

Allocate New Static Public IP

Cancel

Save

Create a VPN Profile

- The profile-based security policy lets you define security rules to a target address, protocol, and ports.
- The default rule for a profile can be configured as deny all or allow all during profile creation.
- This capability allows flexible firewall rules based on the users, instead of a source IP address.

Create Profile

Name

DEVELOPERS-PROFILE

^ Security Policy

Base Policy
☒ Allow All
☐ Deny All

+ Deny Rule

	Target CIDR	Protocol	Port	
1	10.1.1.64/28 ×	ALL × ▼	0:65535	🗑
2	10.1.1.48/28 ×	ALL × ▼	0:65535	🗑
3	10.1.2.48/28 ×	ALL × ▼	0:65535	🗑

User

Cancel Save

Create a VPN User

- After at least one gateway is created, you can add VPN users.
- As soon as a user is created, an email is sent from right away to the recipient, with instructions on how to download client software and connect to a VPN server
- If you would like to assign user profile-based policies, you need to create profiles first

Create VPN User

Name

developer-from-cafe

Email

johndoe@aviatrix.com

VPN Gateway

VPN-GW-LONDON

Base Policy

☒ Allow All ☐ Deny All

Profile

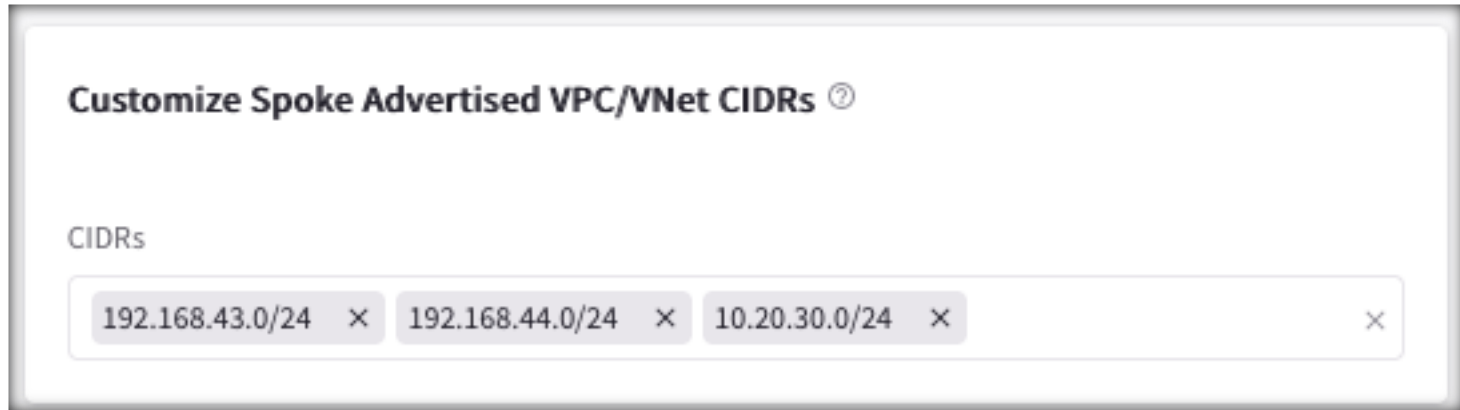
DEVELOPERS-PROFILE

Cancel

Save

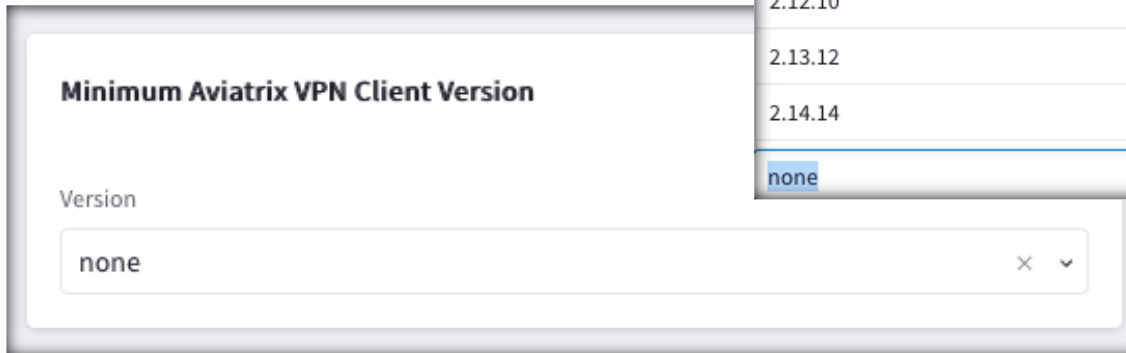
Preserve Client IP

- Client IP can be preserved up to the application
- NAT needs to be disabled on the VPN gateway
- VPN CIDRs must be advertised to the transit for return traffic, from the Spoke Gateway



Minimum Client Version & Duplicate Connections

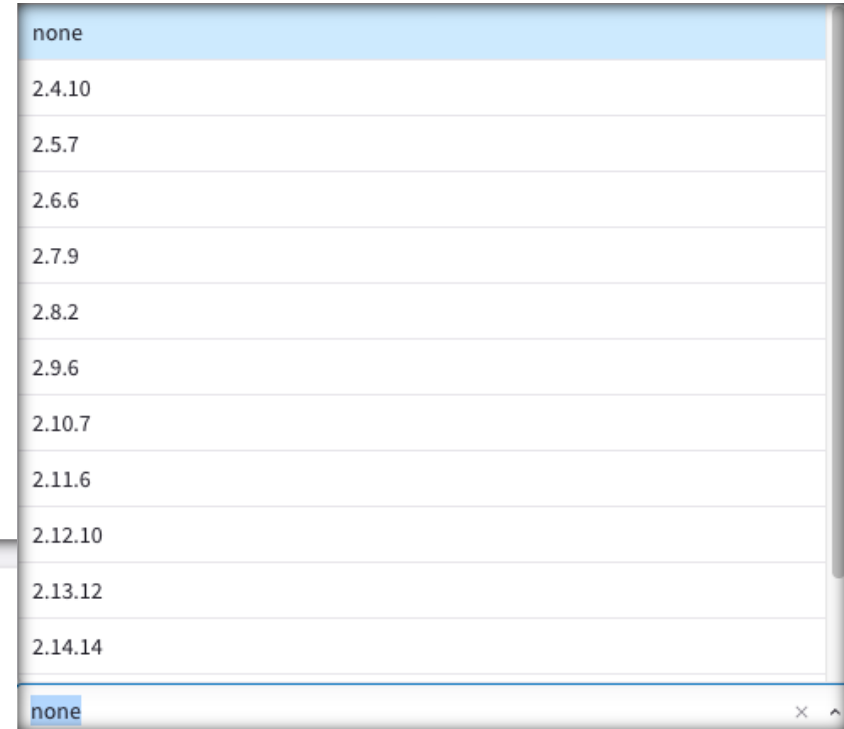
- Enforcement of Minimum VPN Client Version
- Duplicate Connections
 - User can connect simultaneously from multiple devices
 - When disabled, simultaneous sessions are not allowed, and existing VPN connection gets disconnected

A screenshot of a software dialog box titled "Minimum Aviatrix VPN Client Version". It contains a label "Version" and a text input field with the word "none" inside. To the right of the input field are two small icons: a close button (X) and a dropdown arrow (v).

Minimum Aviatrix VPN Client Version

Version

none

A screenshot of a list box containing various version numbers. The list starts with "none" at the top, followed by "2.4.10", "2.5.7", "2.6.6", "2.7.9", "2.8.2", "2.9.6", "2.10.7", "2.11.6", "2.12.10", "2.13.12", and "2.14.14". The "none" option is currently selected and highlighted in blue. The list box has a scrollbar on the right side and a close button (X) and a dropdown arrow (v) at the bottom right.

none
2.4.10
2.5.7
2.6.6
2.7.9
2.8.2
2.9.6
2.10.7
2.11.6
2.12.10
2.13.12
2.14.14

Split Tunnel or Full Tunnel

- **Split Tunnel**

Only specified CIDRs ranges go through the VPN tunnel

- **Full Tunnel**

All user IP sessions including Internet browsing go through the VPN tunnel

Split Tunnel Mode
☒ Yes
☐ No

Additional CIDRs

```
[umair@umair-mbp ~ % ifconfig utun5
utun5: flags=8051<UP,POINTOPOINT,RUNNING,MULTICAST> mtu 1500
        inet 192.168.44.6 --> 192.168.44.5 netmask 0xffffffff
[umair@umair-mbp ~ % netstat -r
Routing tables

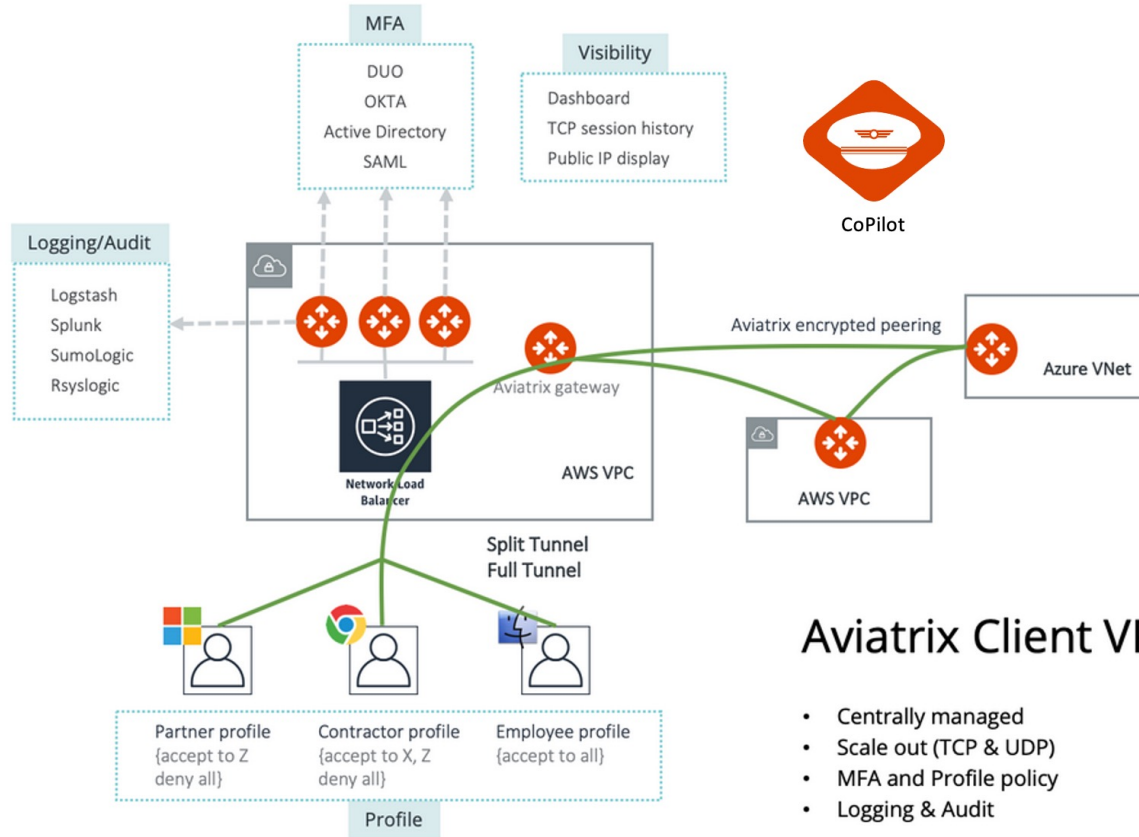
Internet:
Destination            Gateway                Flags                Netif  Expire
default                192.168.1.1           UGScg                en0
10.0.10/24             192.168.44.5         UGSc                 utun5
10.0.20/24             192.168.44.5         UGSc                 utun5
```


Gateway Failover

- Users will automatically get reconnected to another VPN gateway behind the load-balancer
- No change of certificate or user intervention

```
umair@umair-mbp ~ % ifconfig utun4
utun4: flags=8051<UP,POINTOPOINT,RUNNING,MULTICAST> mtu 1500
inet 192.168.43.14 --> 192.168.43.13 netmask 0xffffffff
umair@umair-mbp ~ % ping 10.120.127.191
PING 10.120.127.191 (10.120.127.191): 56 data bytes
64 bytes from 10.120.127.191: icmp_seq=0 ttl=250 time=73.976 ms
64 bytes from 10.120.127.191: icmp_seq=1 ttl=250 time=70.885 ms
64 bytes from 10.120.127.191: icmp_seq=2 ttl=250 time=70.846 ms
64 bytes from 10.120.127.191: icmp_seq=3 ttl=250 time=60.916 ms
64 bytes from 10.120.127.191: icmp_seq=4 ttl=250 time=67.720 ms
64 bytes from 10.120.127.191: icmp_seq=5 ttl=250 time=61.405 ms
64 bytes from 10.120.127.191: icmp_seq=6 ttl=250 time=61.982 ms
Request timeout for icmp_seq 7
Request timeout for icmp_seq 8
Request timeout for icmp_seq 9
Request timeout for icmp_seq 10
Request timeout for icmp_seq 11
Request timeout for icmp_seq 12
Request timeout for icmp_seq 13
Request timeout for icmp_seq 14
Request timeout for icmp_seq 15
Request timeout for icmp_seq 16
Request timeout for icmp_seq 17
Request timeout for icmp_seq 18
Request timeout for icmp_seq 19
64 bytes from 10.120.127.191: icmp_seq=20 ttl=250 time=72.759 ms
64 bytes from 10.120.127.191: icmp_seq=21 ttl=250 time=63.880 ms
64 bytes from 10.120.127.191: icmp_seq=22 ttl=250 time=67.266 ms
64 bytes from 10.120.127.191: icmp_seq=23 ttl=250 time=66.668 ms
64 bytes from 10.120.127.191: icmp_seq=24 ttl=250 time=68.084 ms
^C
--- 10.120.127.191 ping statistics ---
25 packets transmitted, 12 packets received, 52.0% packet loss
round-trip min/avg/max/stddev = 60.916/67.199/73.976/4.246 ms
umair@umair-mbp ~ % ifconfig utun4
utun4: flags=8051<UP,POINTOPOINT,RUNNING,MULTICAST> mtu 1500
inet 192.168.44.6 --> 192.168.44.5 netmask 0xffffffff
umair@umair-mbp ~ %
```

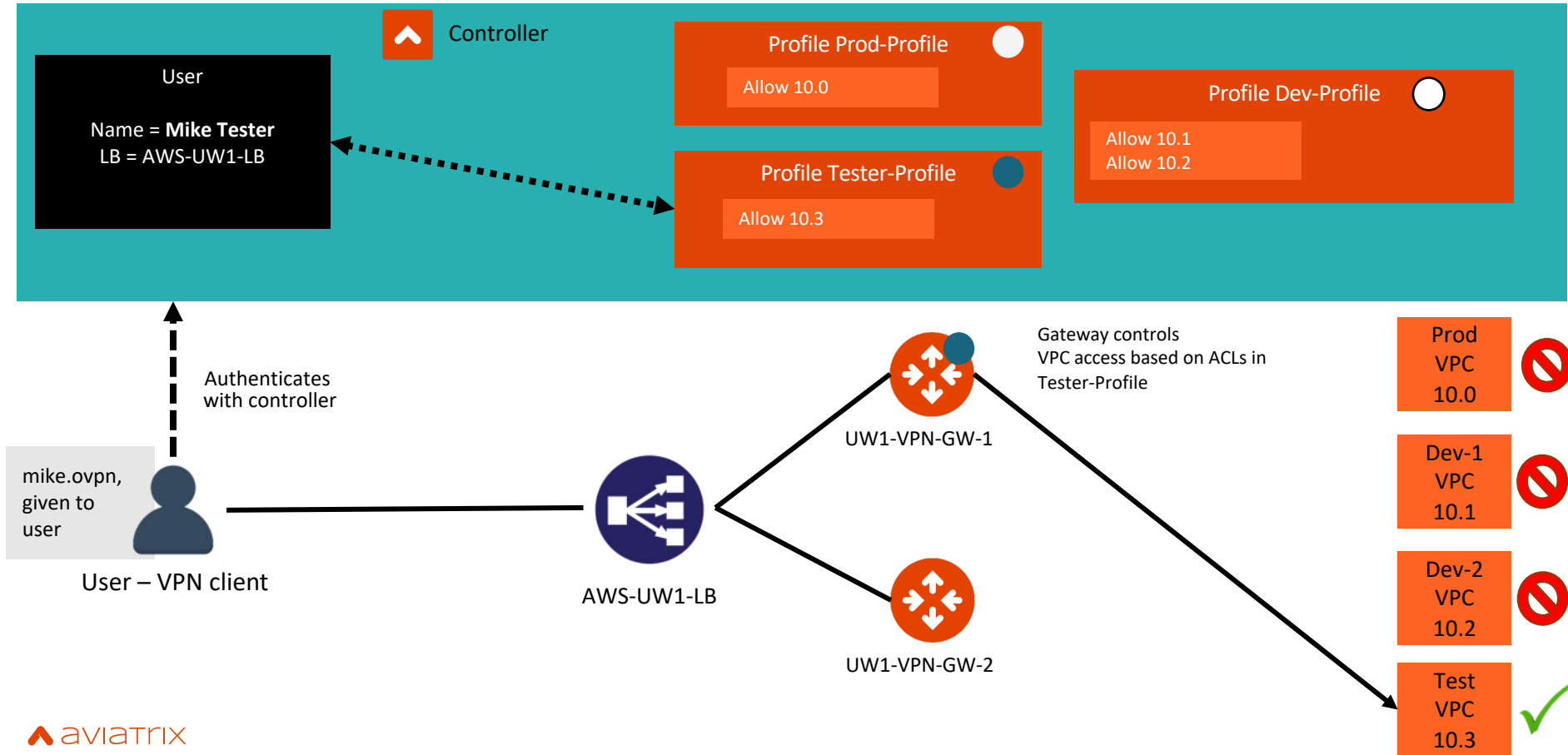
UserVPN Reference Architecture



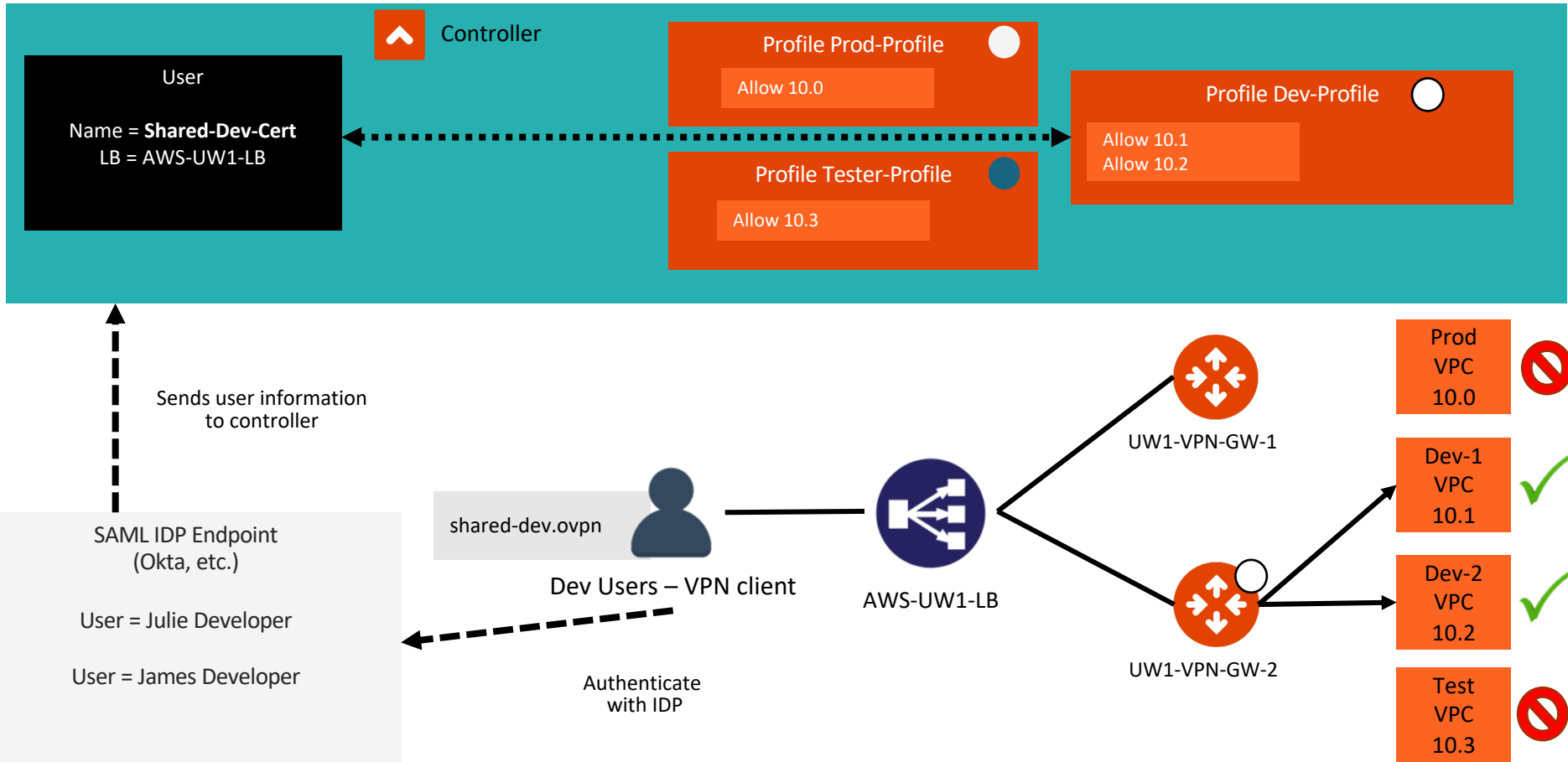
Aviatrix Client VPN Solution

- Centrally managed
- Scale out (TCP & UDP)
- MFA and Profile policy
- Logging & Audit

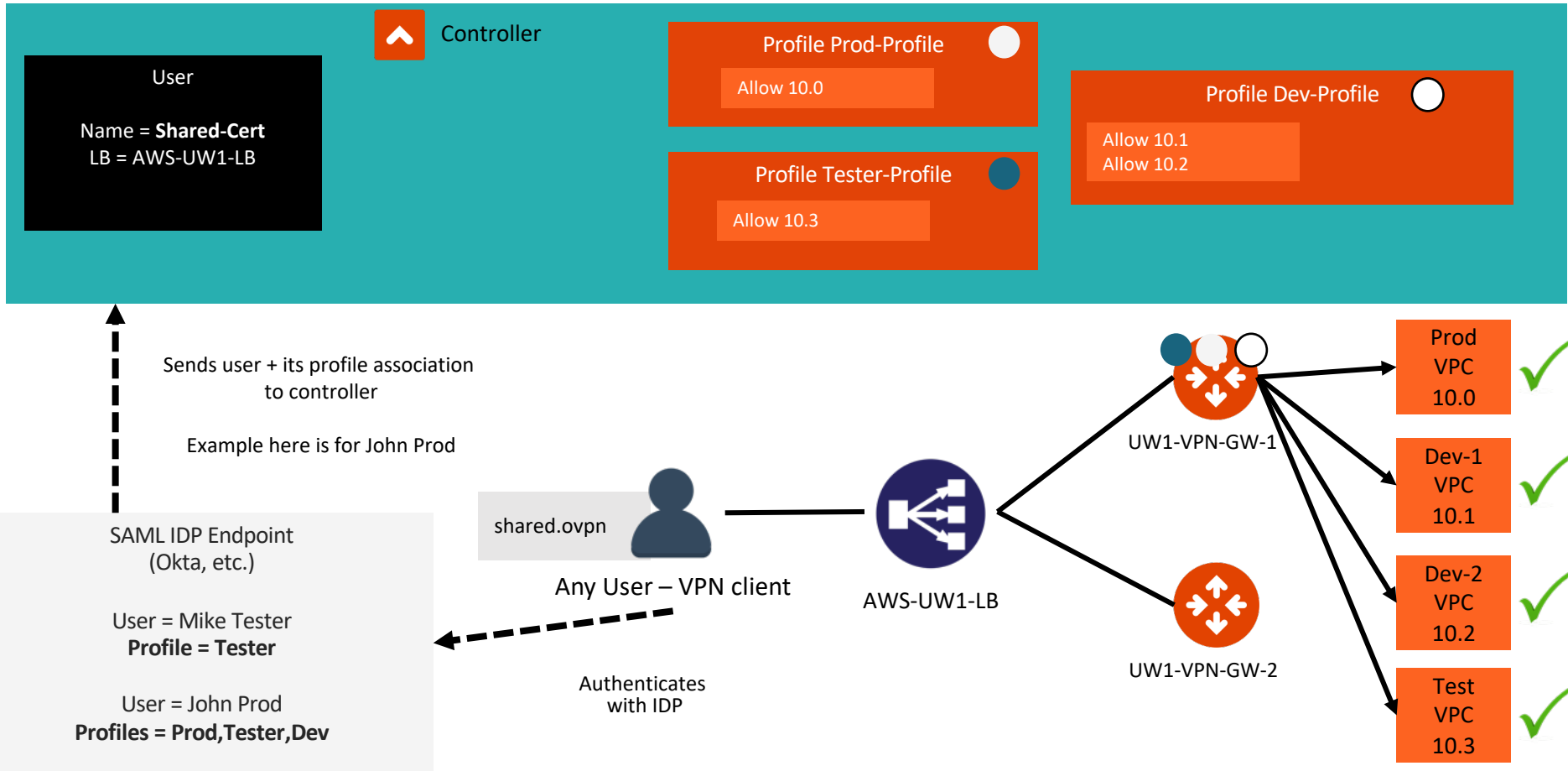
Users and Profiles



Users in IDP, Profile Association in Controller



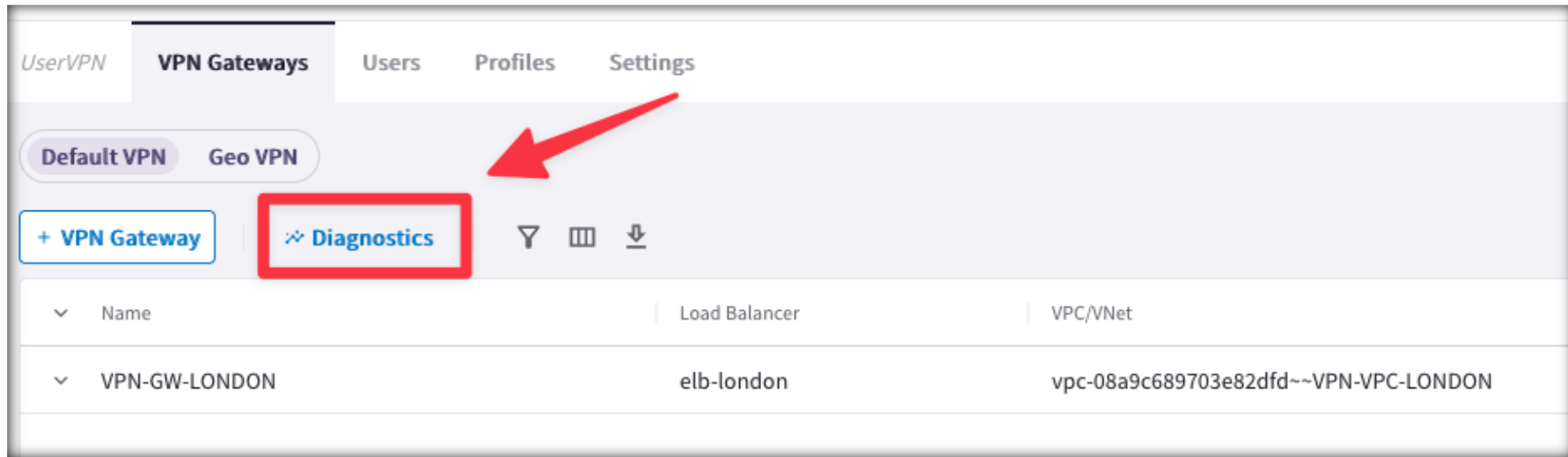
Users in IDP, Profile Association in IDP Profile as SAML Attribute





Visibility and Troubleshooting

User VPN Diagnostics Tools



- Use the UserVPN Diagnostics tool to check a VPN gateway's performance and connectivity

Diagnostics

- **Diagnostics Tab:** to run diagnostics on a VPN user to check their connectivity and performance
- **Session History Tab:** to review specific VPN gateway sessions in more detail
- **ELB Status Tab:** to check on the status of load balancers within specific VPCs/VNet

UserVPN Diagnostics Tools:

Tools ☰ <

Diagnostics

Session History

ELB Status

Last Run: Feb 28, 2024 10:23 PM

User's Name

developer-from-cafe

Run

```
VPN-GW-LONDON    2024-02-28T21:19:48.960469+00:00 GW-VPN-GW-LONDON-13.42.189.54
openvpn[12807]: 31.165.116.229:4553 VERIFY OK: depth=0, C=US, ST=CA, L=SantaClara, O=Aviatix,
OU=Engineering, CN=developer-from-cafe, name=server, emailAddress=info@aviatrix.com
```




aviatrix

ACE

**Aviatrix Certified
Engineer**