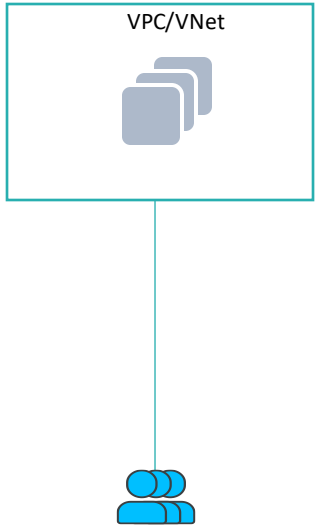
User VPN

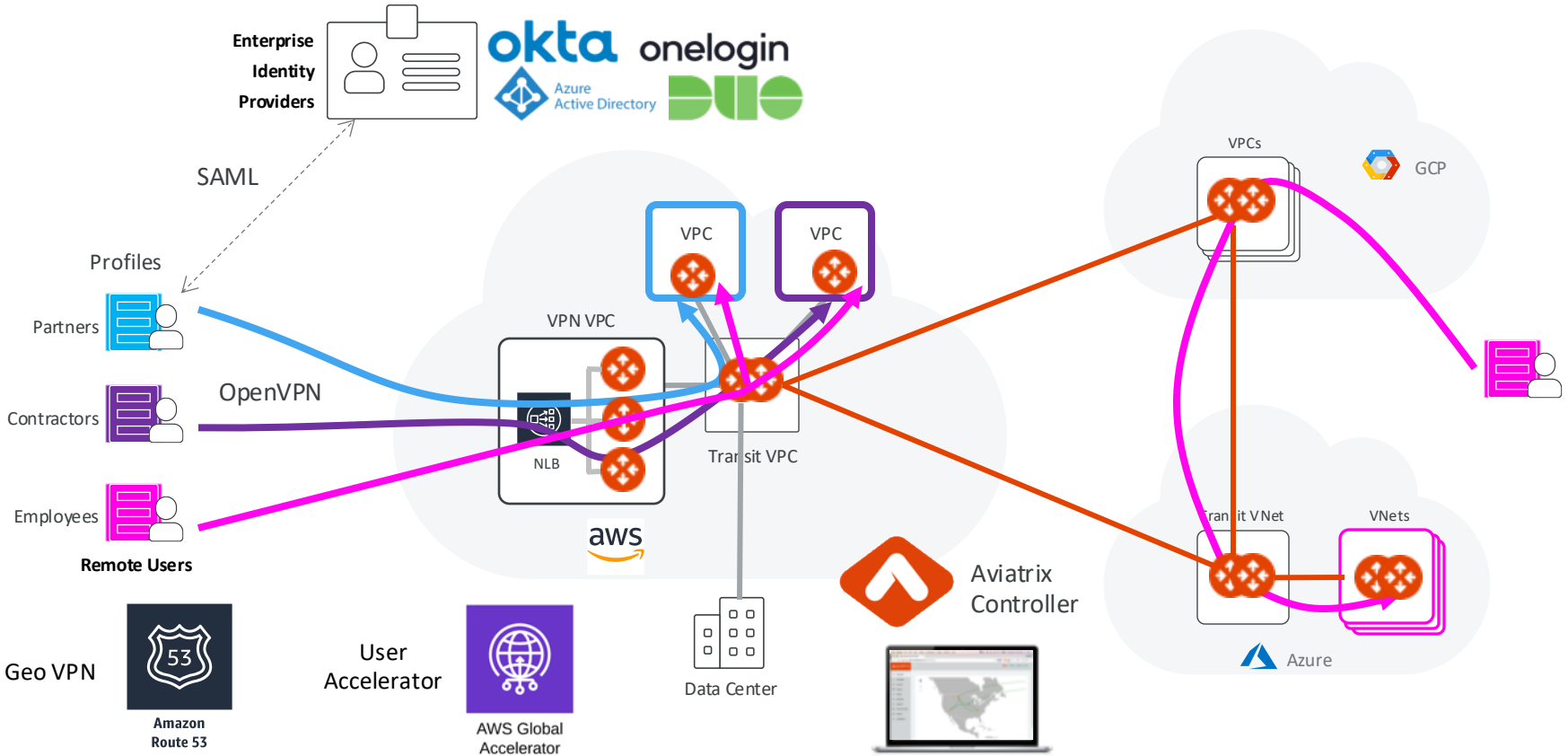
ACE Team

Problem Statement

- Connect users/partners/developers 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

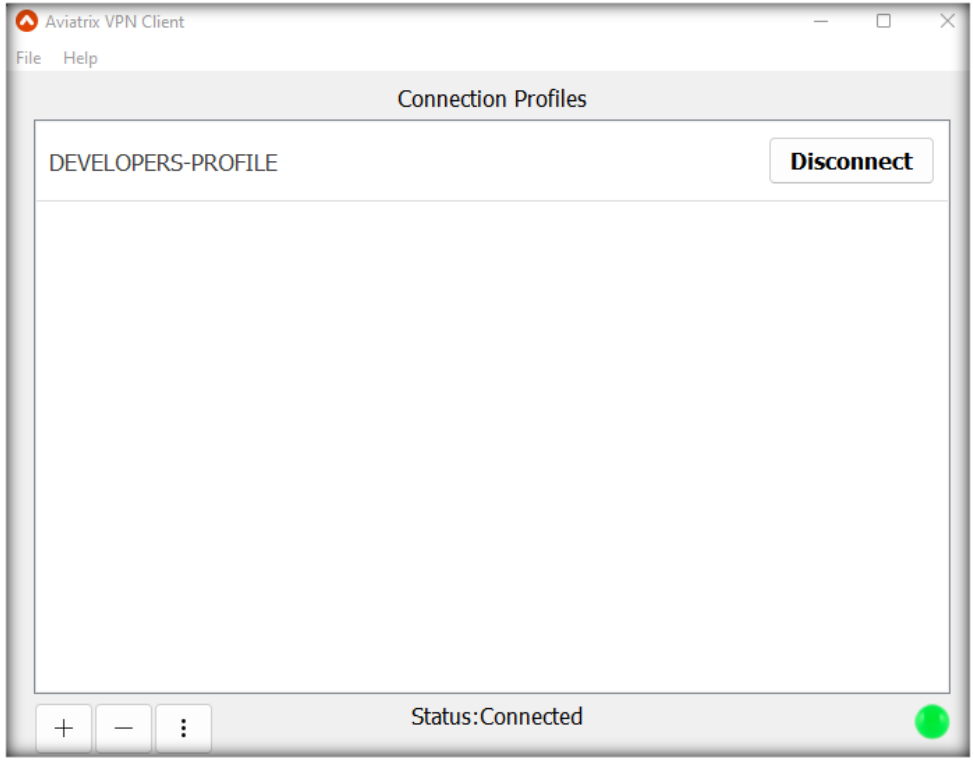


User VPN Overview



Client Software

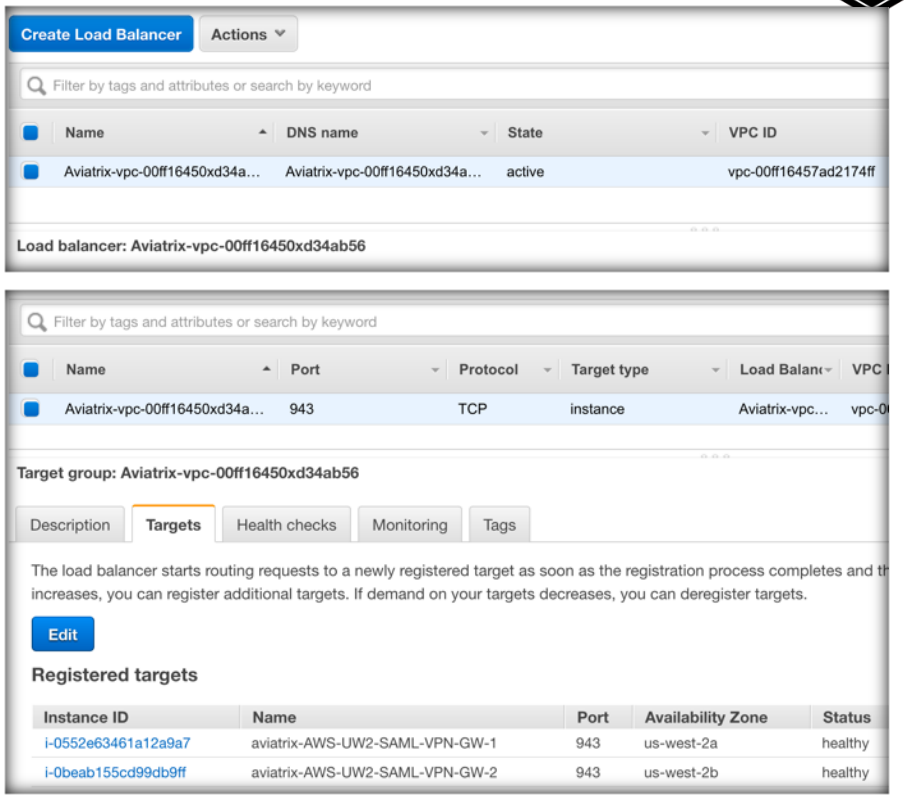
- OpenVPN Client
  - All OpenVPN client software are supported. The supported clients are macOS, Windows iOS, Android, Chromebook, Linux and BSD
- Aviatrix VPN Client
  - Aviatrix VPN Client supports macOS, Windows, Linux Debian distribution, and BSD distribution
  - Choose Aviatrix VPN Client if you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



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

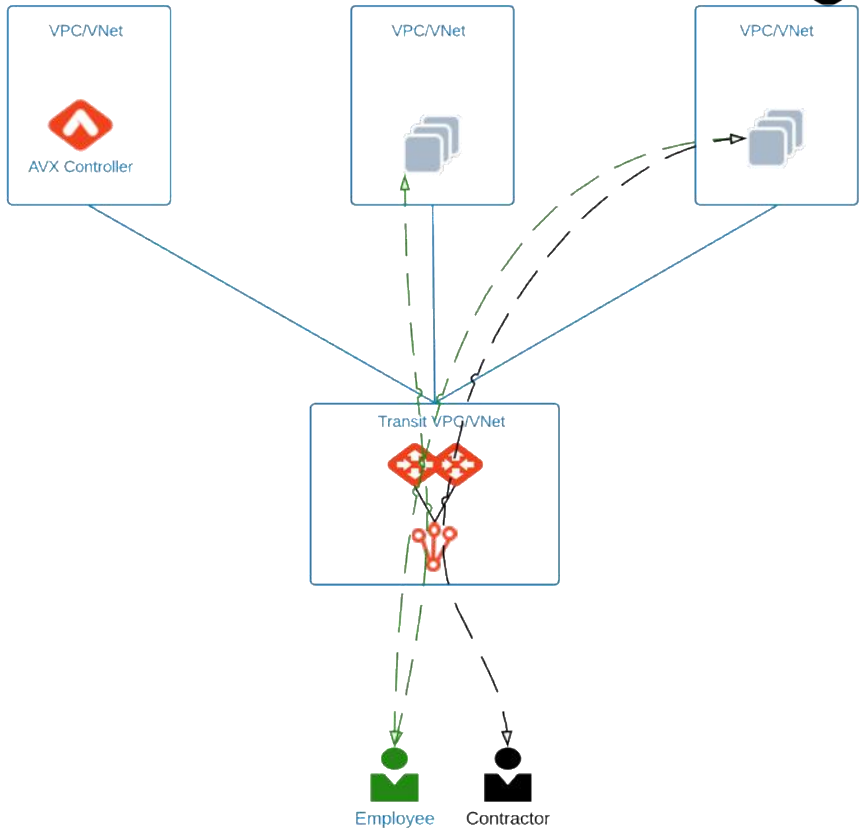
Automated Load Balancer

- 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



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



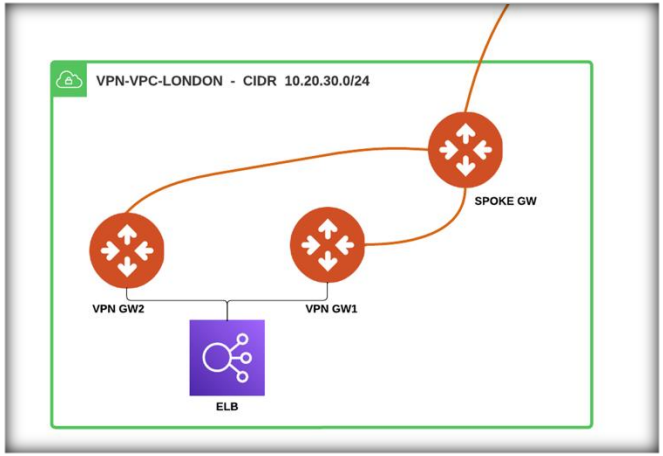
Secure Assertion Markup Language

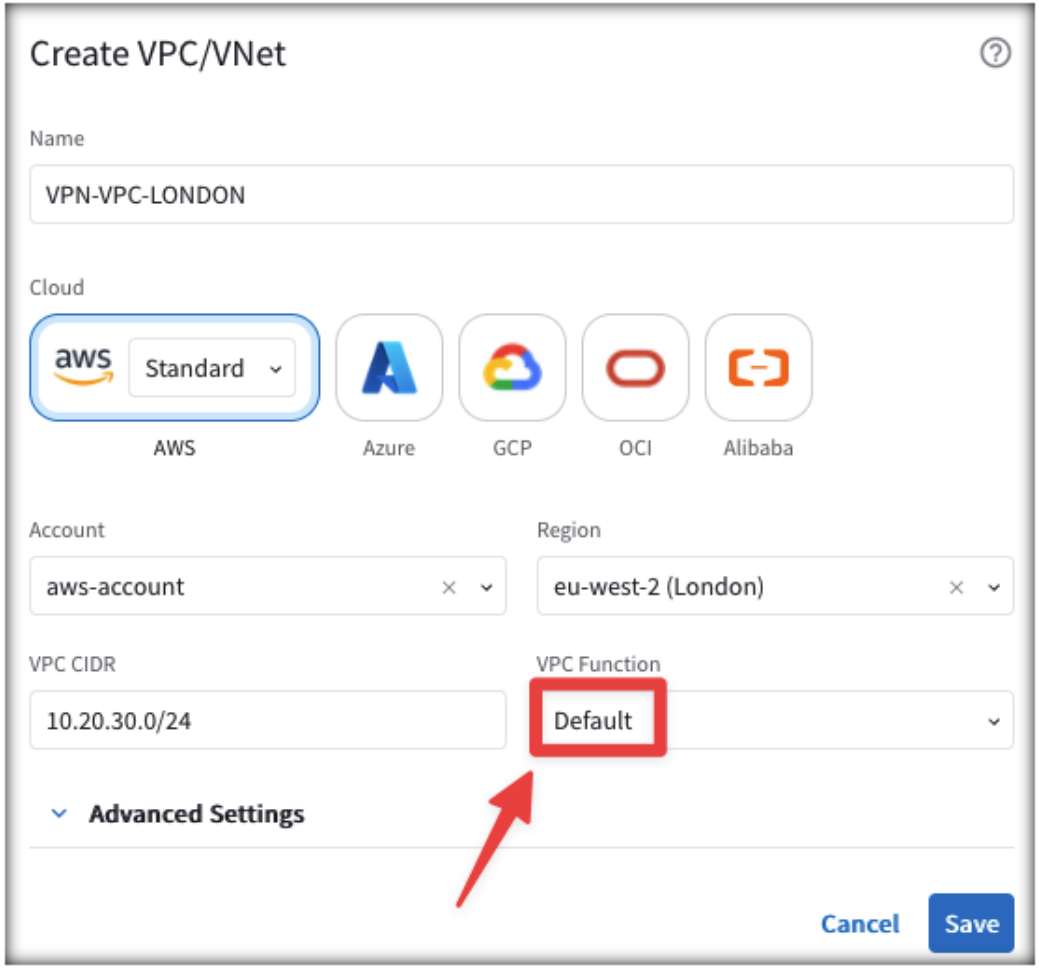
- Supports IDPs like Azure AD, Okta, Duo, Office 365
- User accounts are onboarded on the IDP portal
- Users can be onboarded on Aviatrix controller if SAML is not required

AWS SSO

Ad-hoc VPN VPC

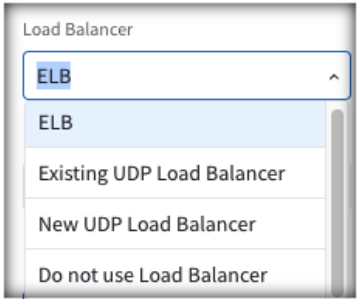
- Crate a dedicated VPC
  - Select the **Default** VPC (i.e. Spoke VPC)
- This VPC will host the User-VPN Gateways, the ELB and the Spoke Gateways

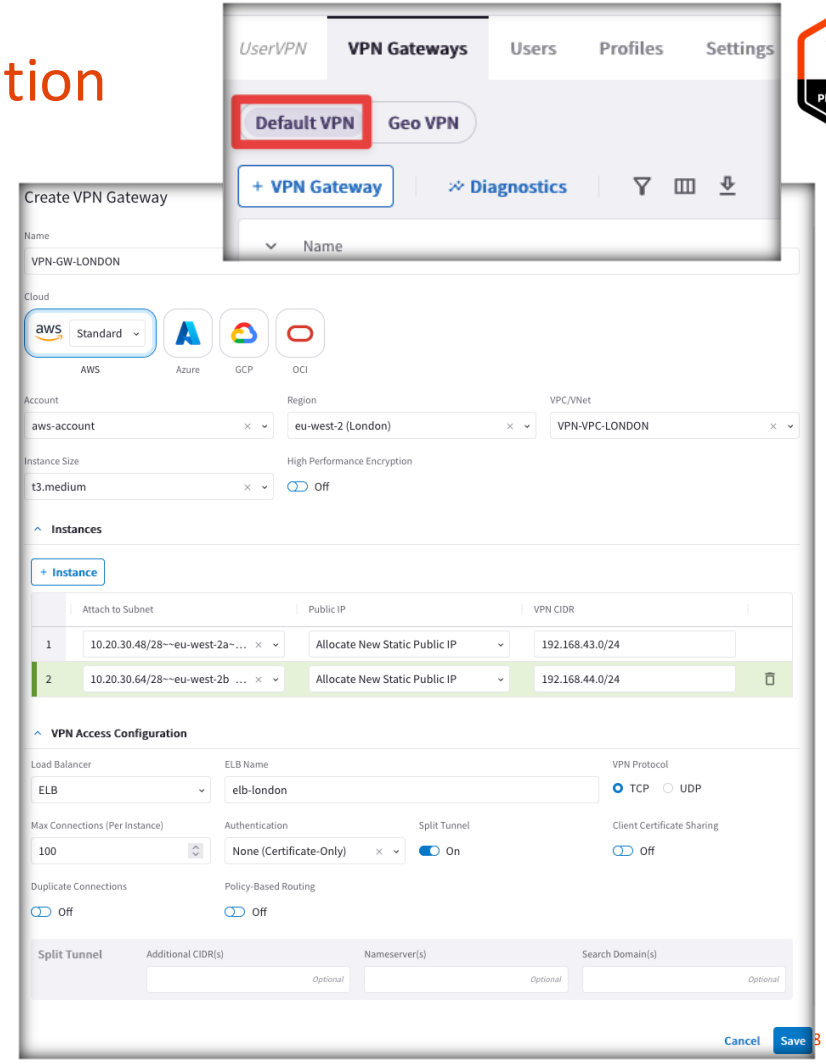




Default VPN Gateways and ELB Creation

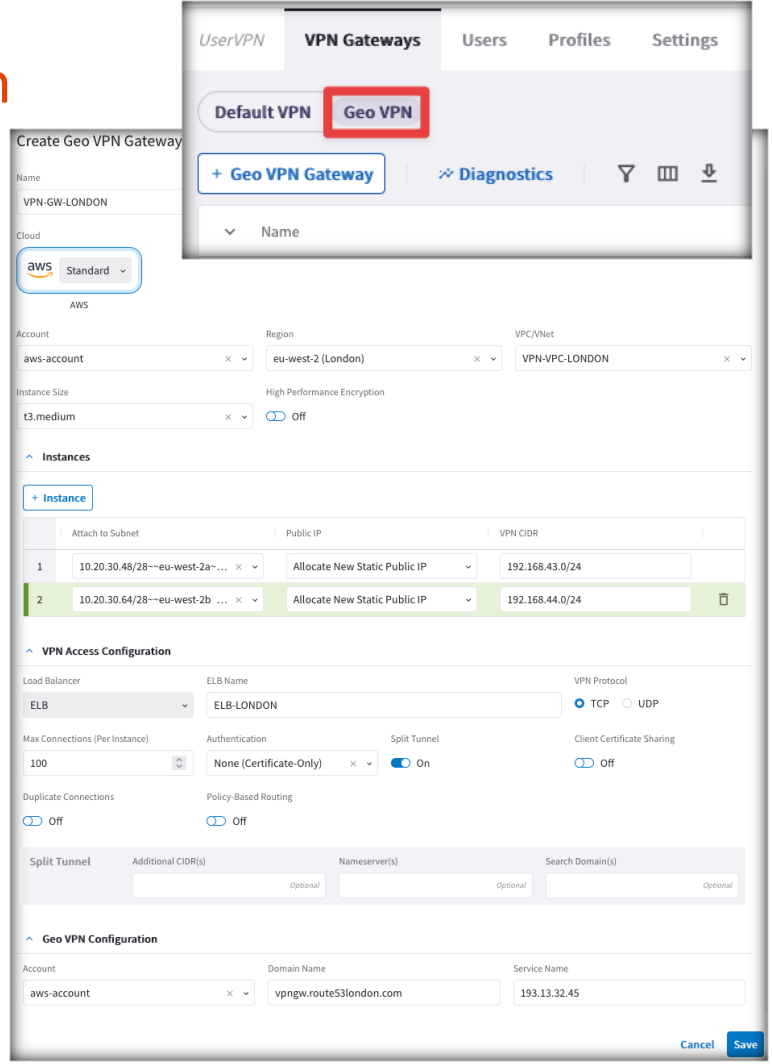
- Configure one or more VPN Gateways
  - Each VPN Gateway must be configured with its own **VPN CIDR Block**
  - When a VPN user connects to the VPN gateway, the user will be assigned a virtual IP address from the VPN CIDR Block
  - The default IP address pool is **192.168.43.0/24**
- The ELB template 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**





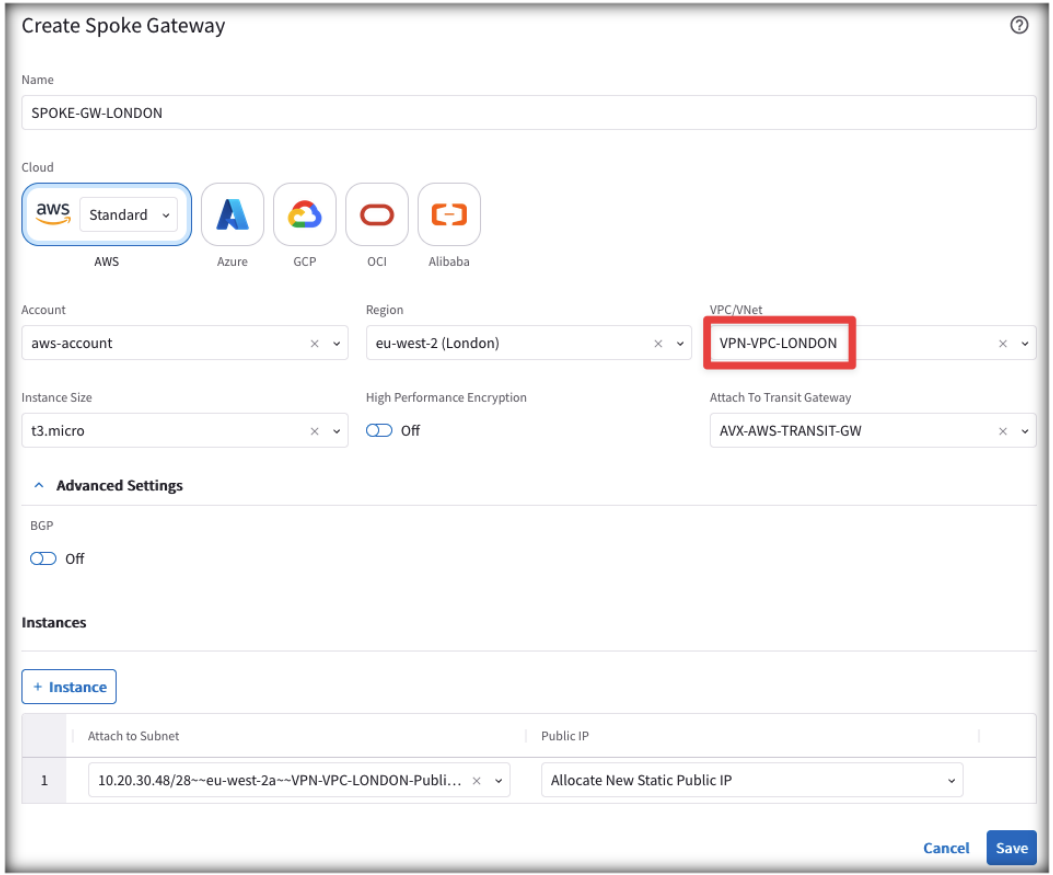
Geo VPN Gateways and ELB Creation

- 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



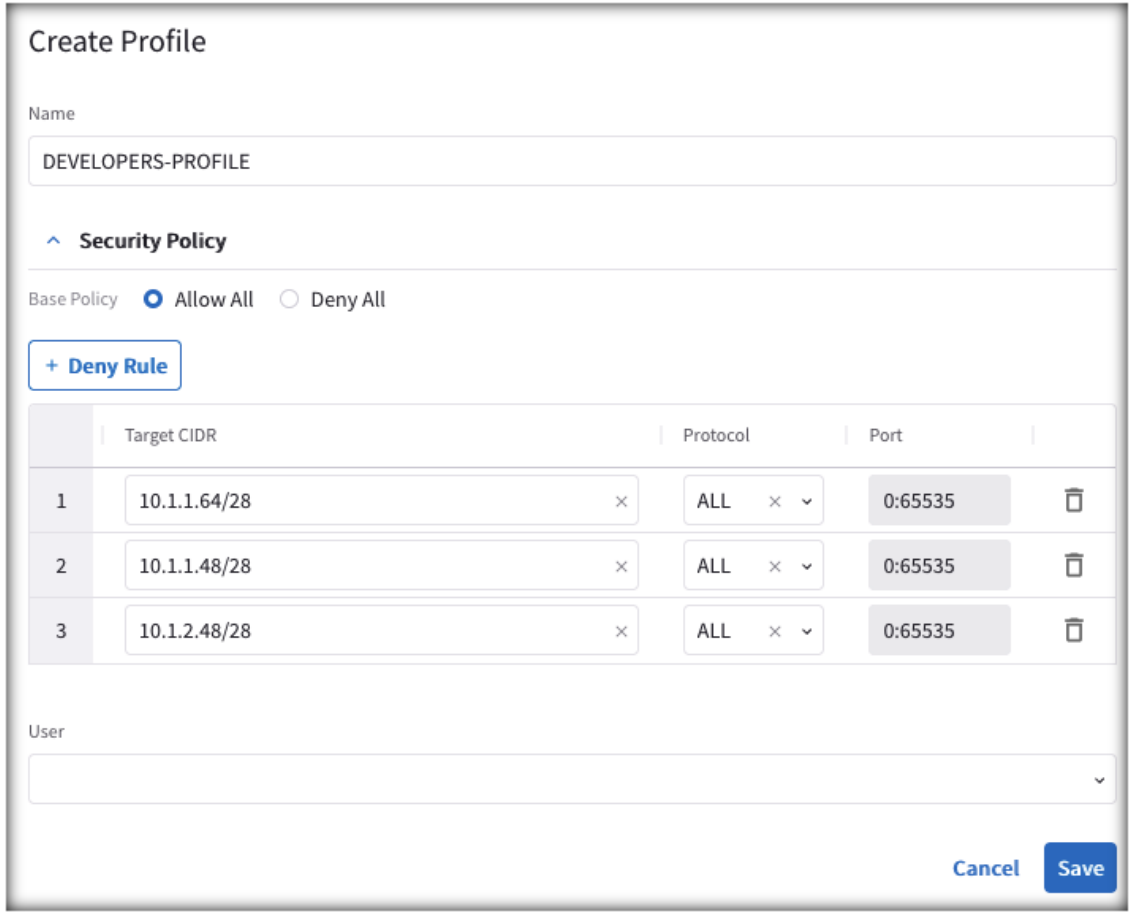
Create the Spoke GW inside the VPN VPC

- 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



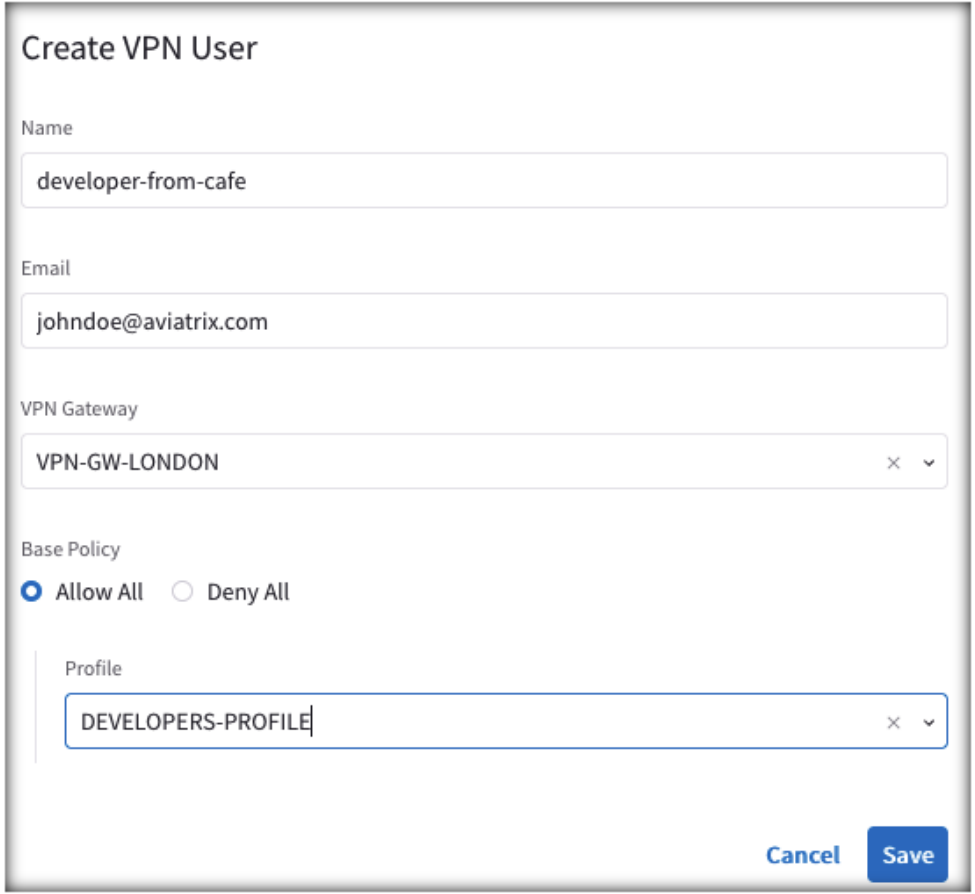
Create a VPN Profile

- 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 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

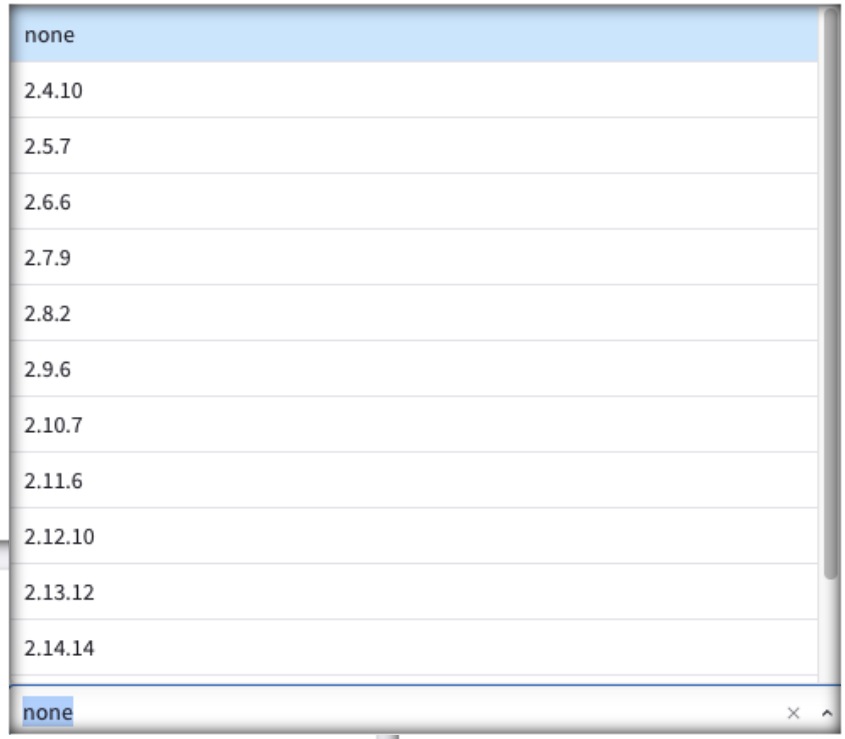


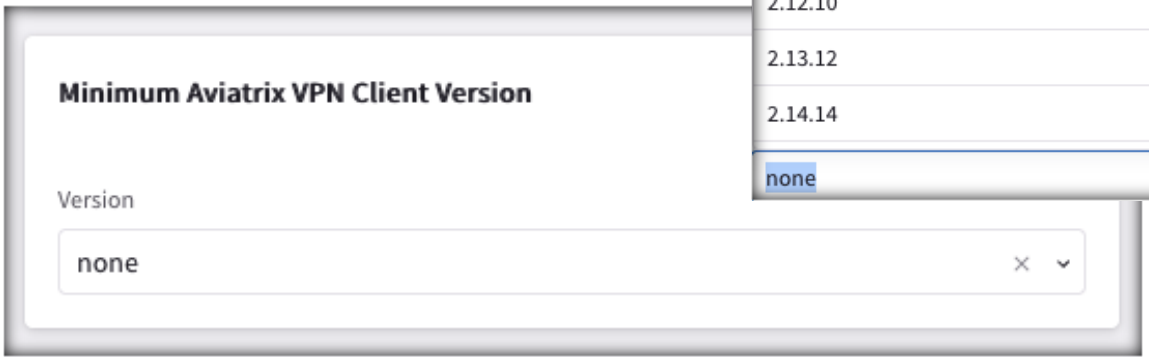
Preserve Client IP

- 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





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

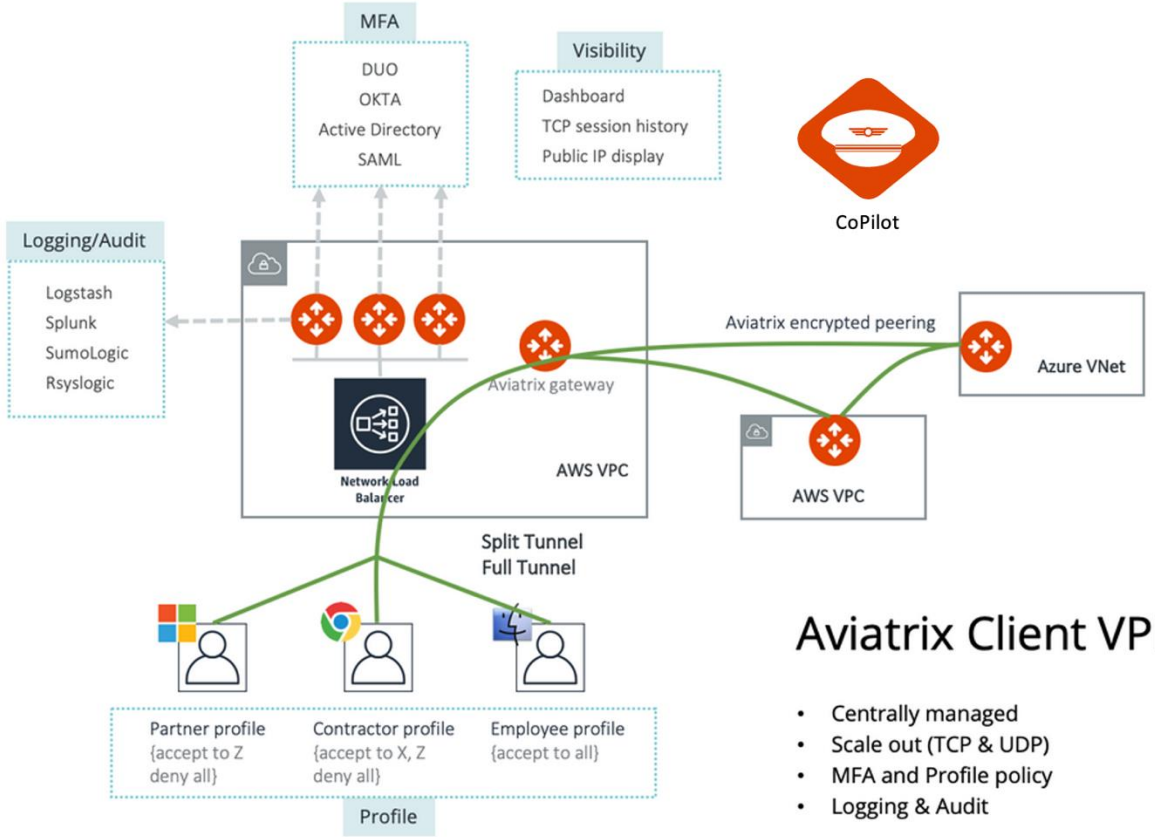

```
[umair@umair-mbp ~ % ifconfig utun5
utun5: flags=8051<UP,POINTOPOINT,RUNNING,MULTICAST> mtu 1500
        inet 192.168.44.6 --> 192.168.44.5 netmask 0xffffffff
[umair@umair-mbp ~ % netstat -r
Routing tables

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

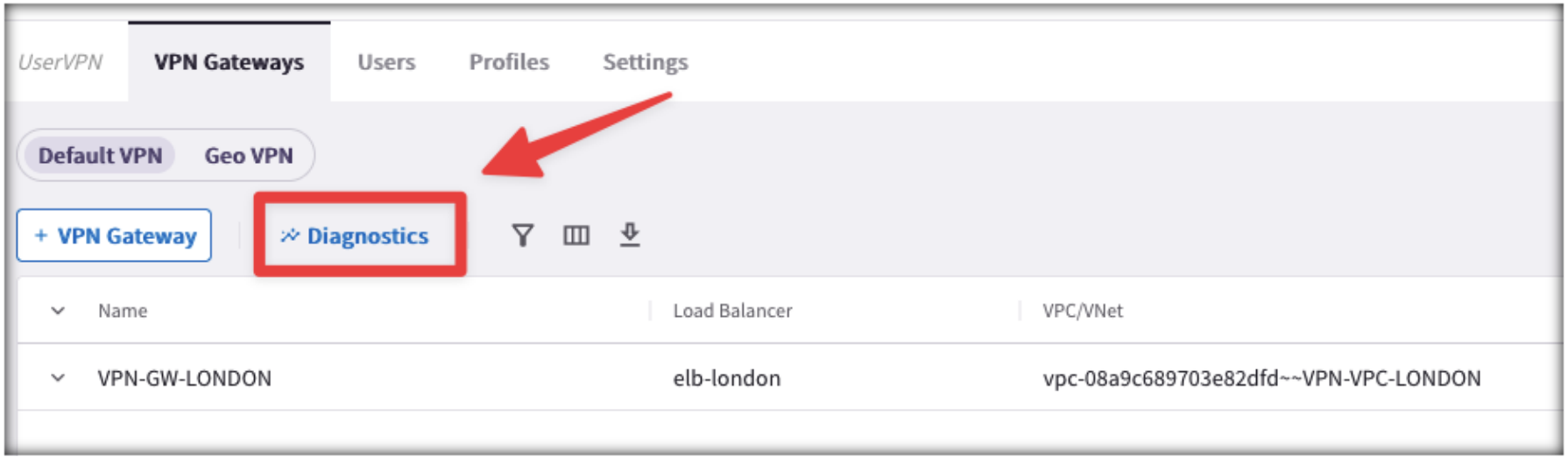


Aviatrix Client VPN Solution

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

Visibility and Troubleshooting

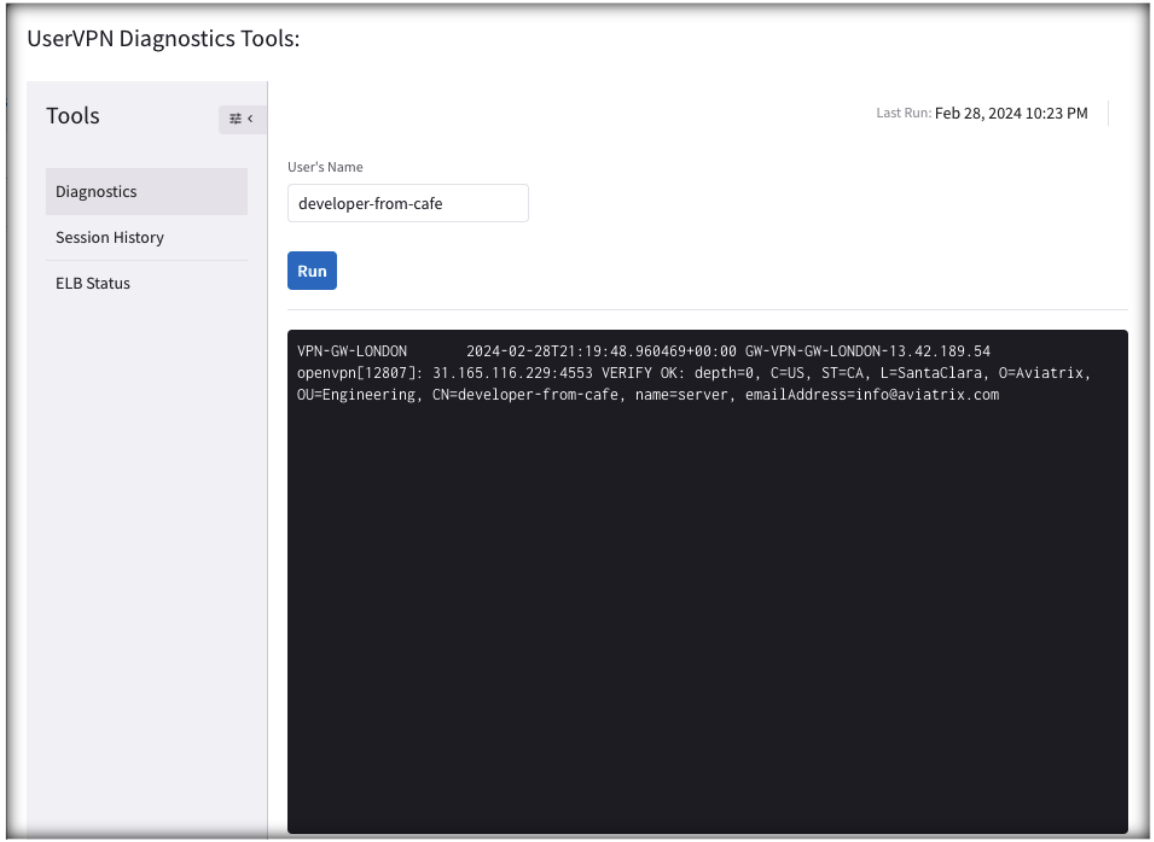
User VPN Diagnostics Tools



- 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



Next: Lab 7 – Site2Cloud
Lab 8 – Aviatrix Edge