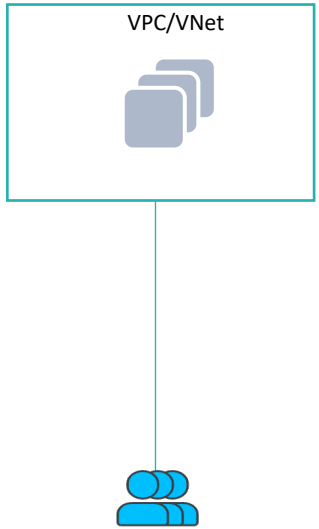
User VPN

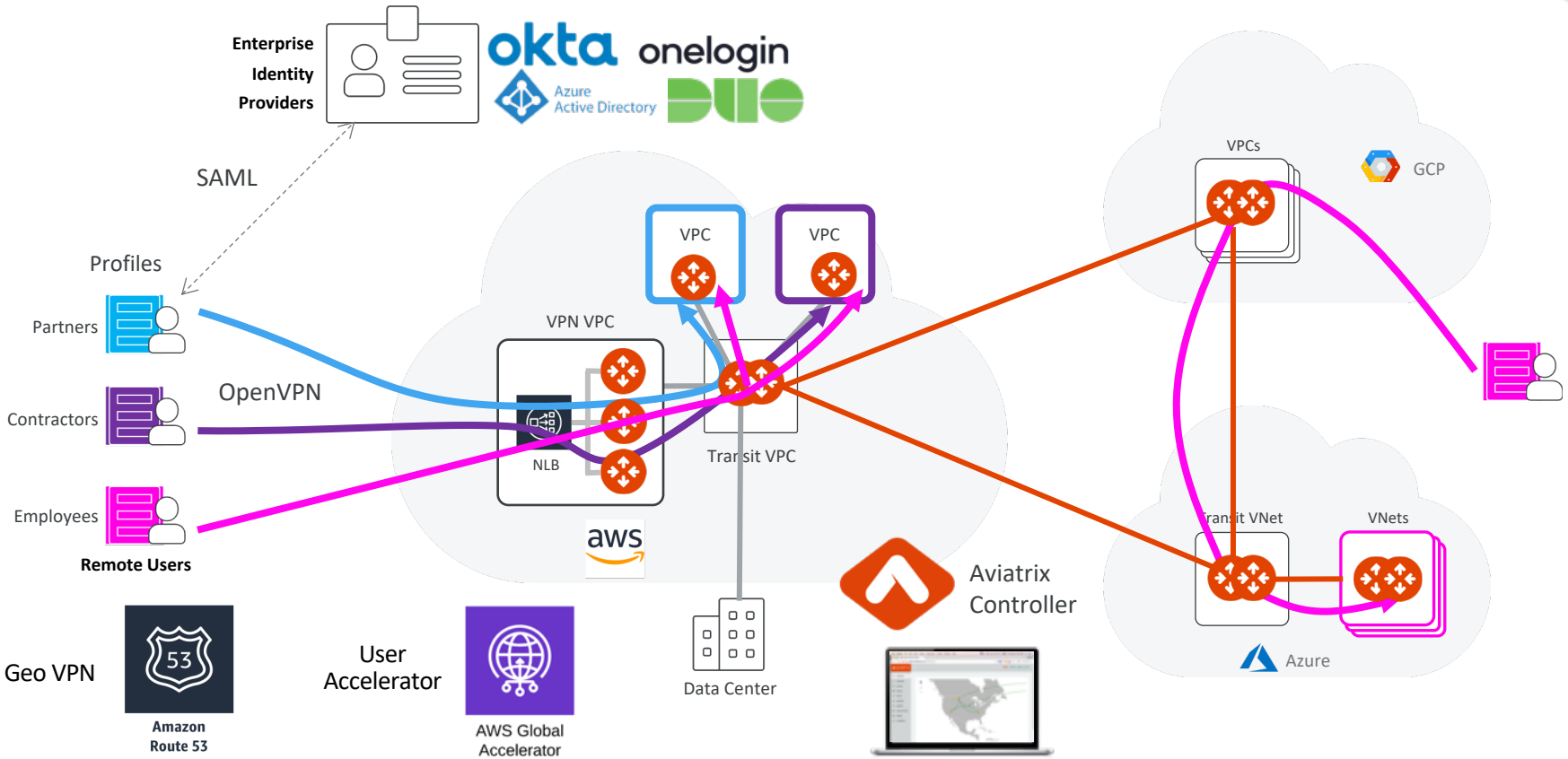
ACE Solutions Architecture Team

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

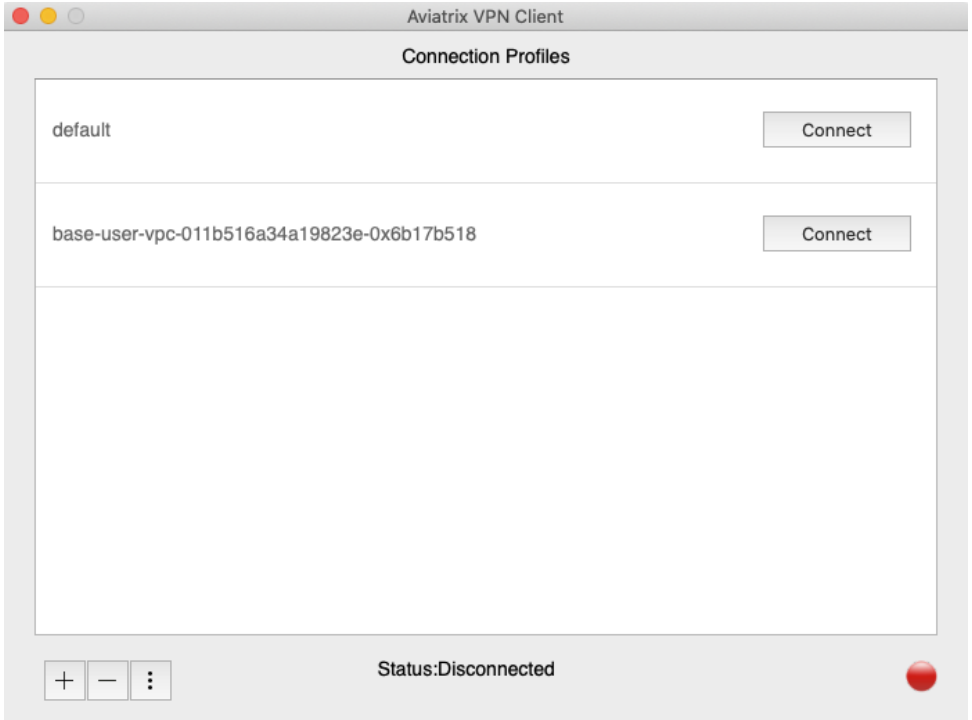


User VPN Overview



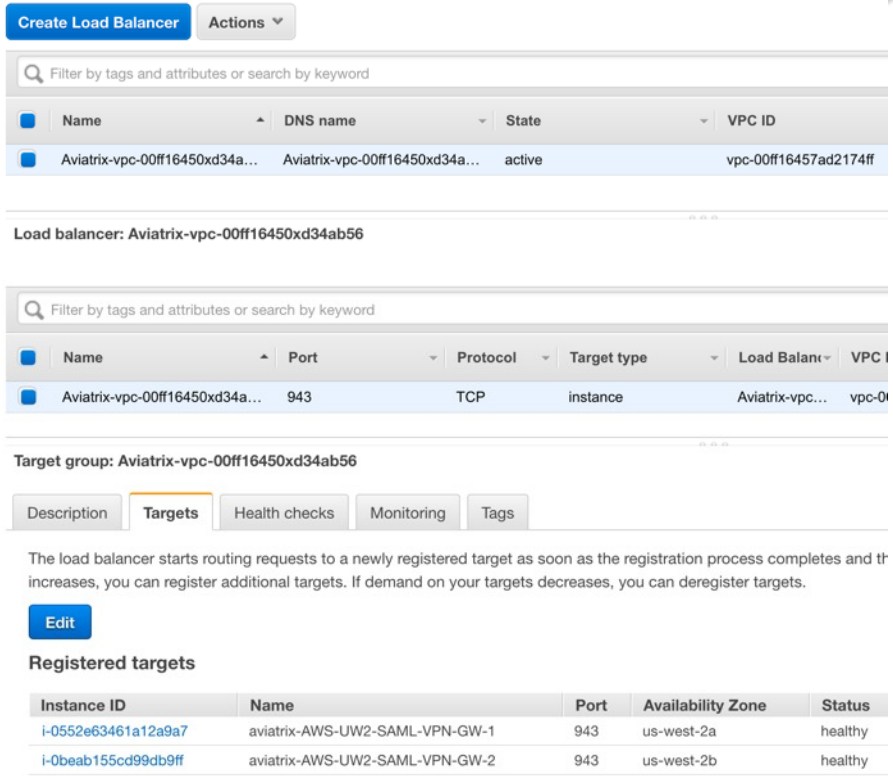
Client Software

- 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



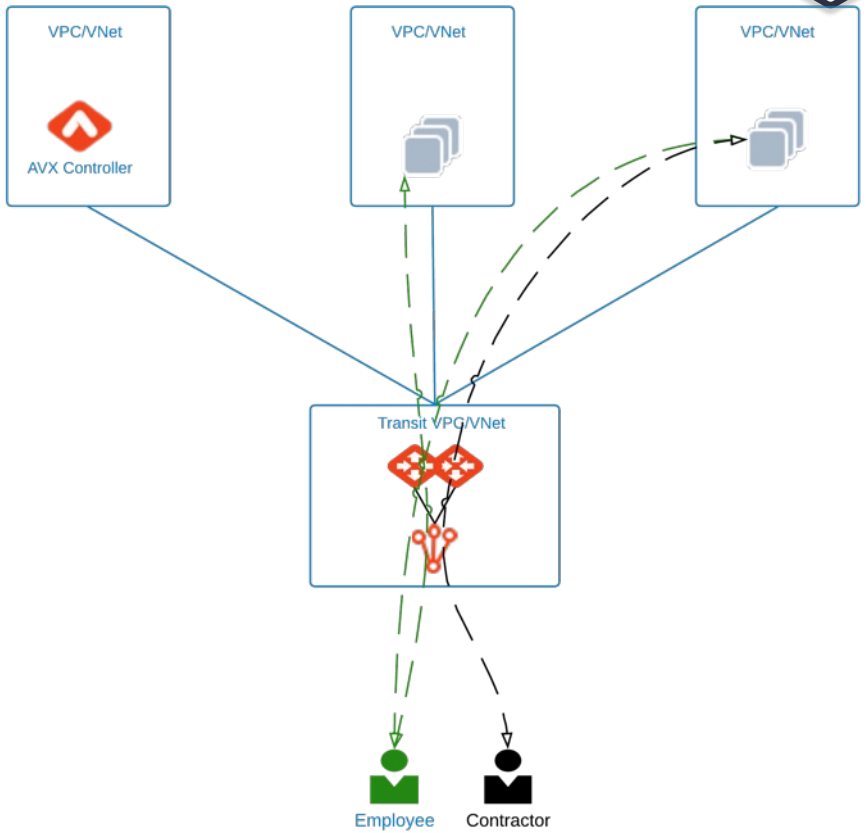
Automated Load Balancer

- 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

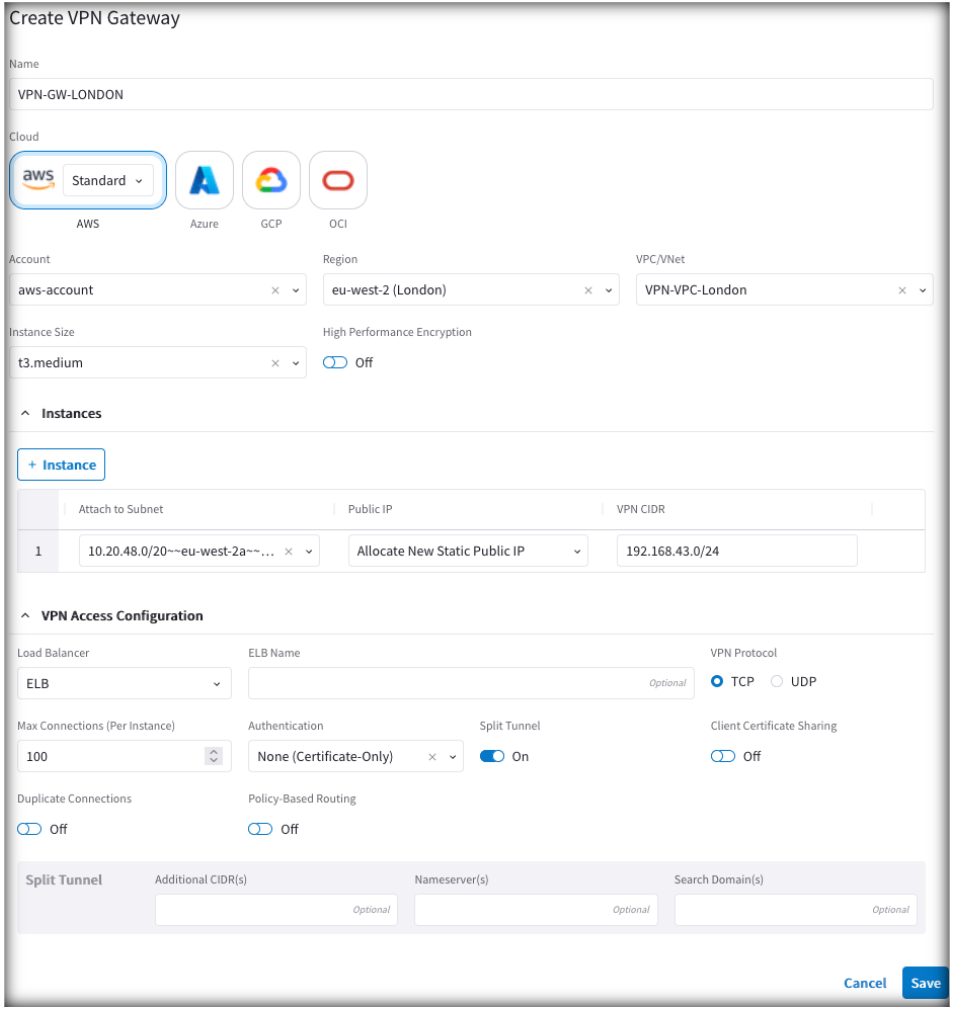


Secure Assertion Markup Language

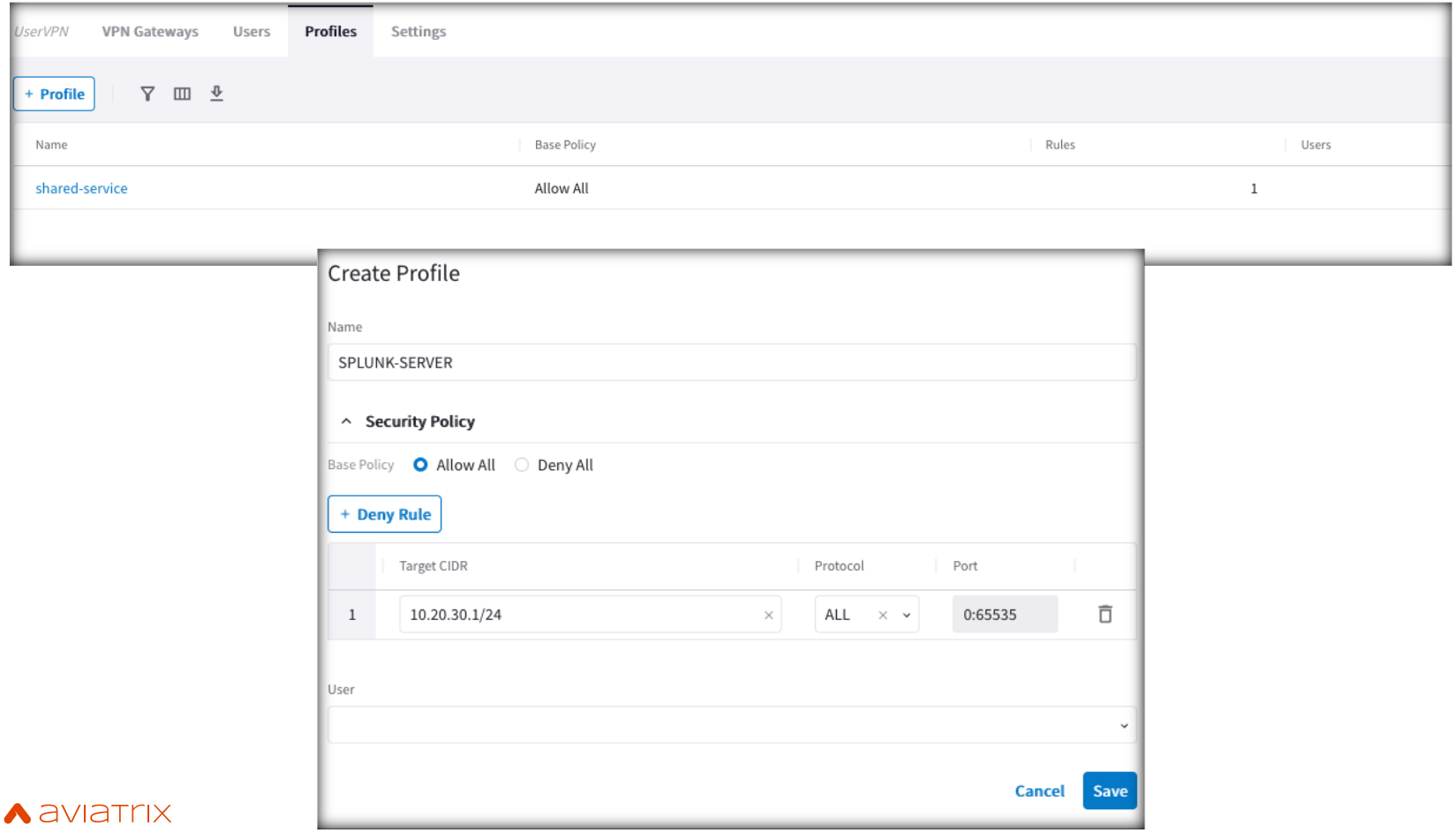
- Supports IDPs like Azure AD, Okta, Duo, Office 365
- User accounts are onboarded on the IDP portal
- Users can be onboarded on Aviatrix controller if SAML is not required

AWS SSO

VPN Gateway Creation

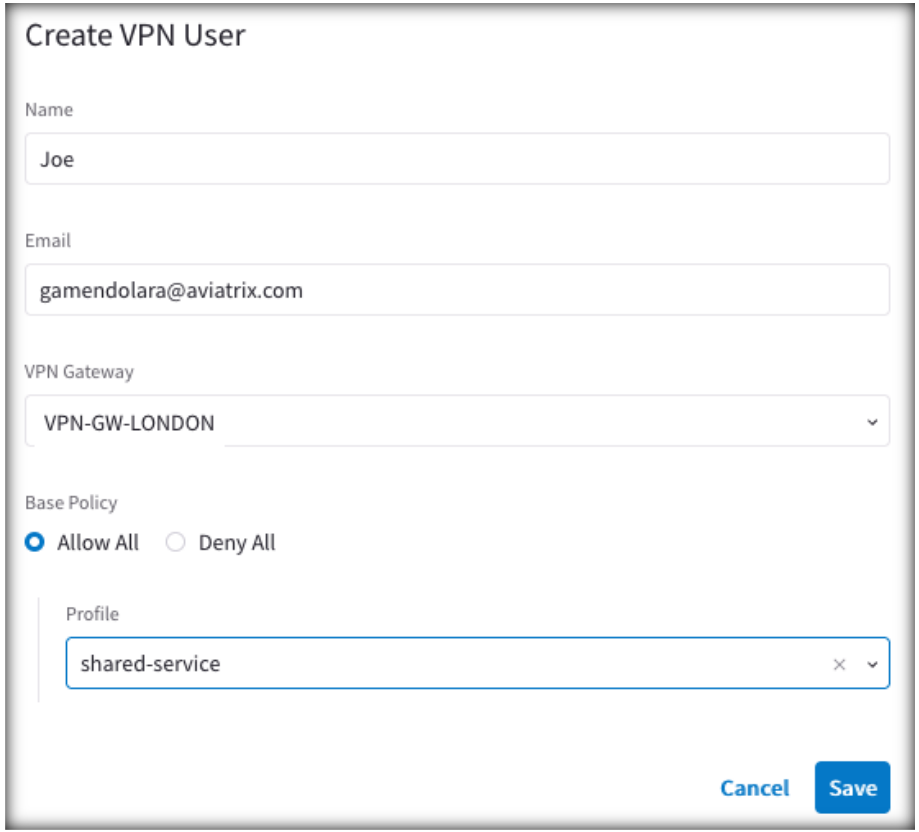


Profiles


UserVPN
VPN Gateways
Users
Profiles
Settings
+ Profile
Name
Base Policy
Rules
Users
shared-service
Allow All
1
Create Profile
Name
SPLUNK-SERVER
Security Policy
Base Policy
Allow All
Deny All
+ Deny Rule
Target CIDR
Protocol
Port
1
10.20.30.1/24
ALL
0:65535
User
Cancel
Save

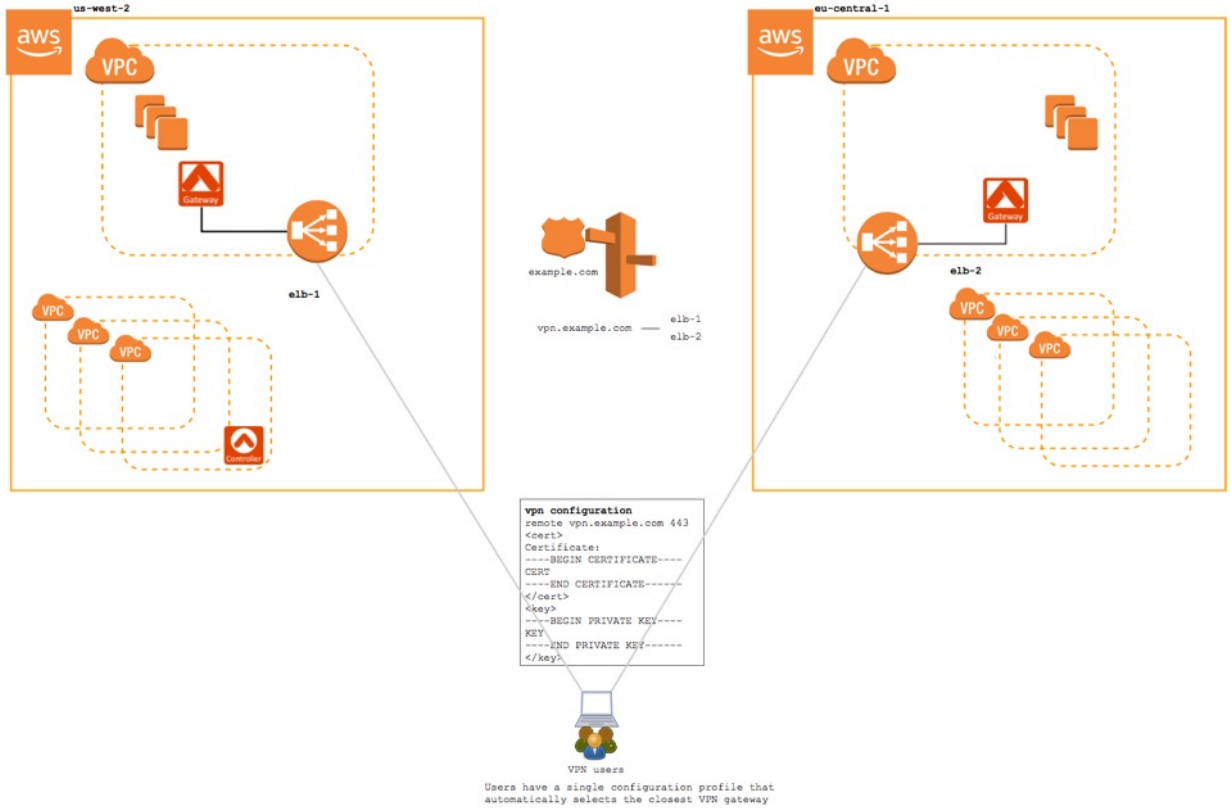
Profiles ←→ Users

- A profile can be associated with multiple users.
- A user can be associated with multiple profiles.



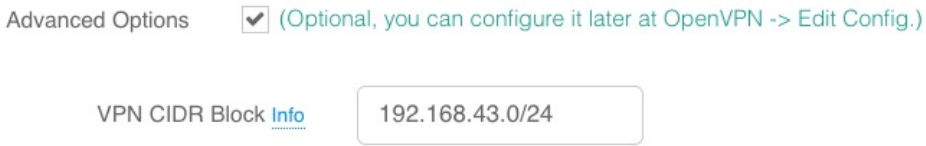
Geo VPN – VPN User Accelerator

- Combines the Aviatrix scale-out VPN solution with latency-based routing to dynamically route VPN users to the nearest Aviatrix VPN gateway based on the latency between the user and the gateways
- Users are directed to an Amazon Route 53 DNS or Azure DNS, that uses a latency-based routing policy to choose between the available regions



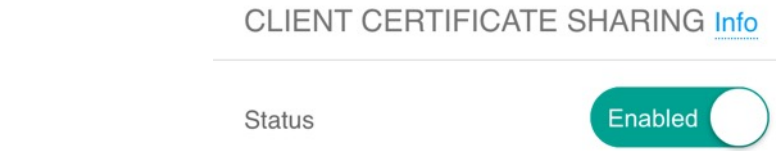
Custom VPN CIDR Block

- The default IP address pool is 192.168.43.0/24
- This is a configurable parameter



Client Certificate Sharing

- Disabled by default
- Multiple VPN users can share the same .ovpn file
- Can only be used when authenticating users via IDP
- The controller still sees individual users and maintains full history



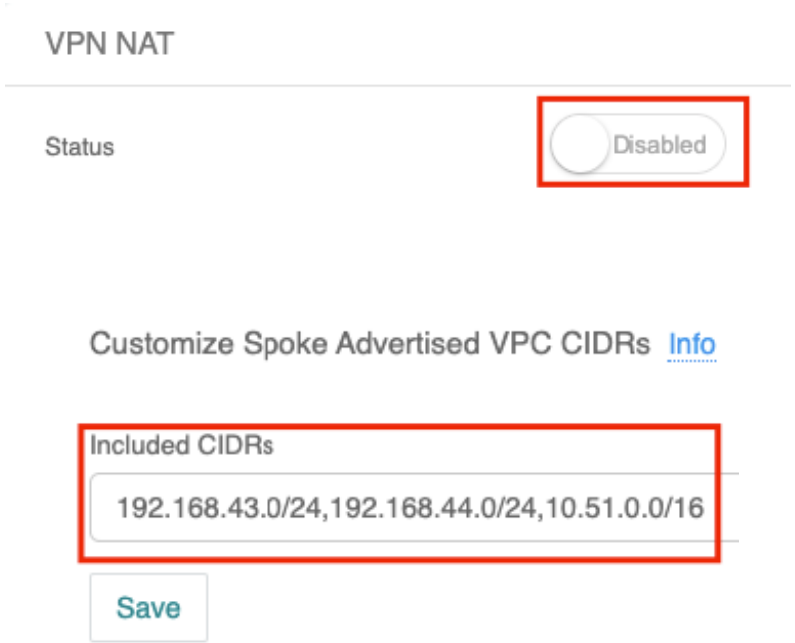
ACTIVE VPN USERS TOTAL: 2

Search history

Name	Profile	Virtual IP	Landing Gate…	Login Time	Public IP
julie@abc.com	Developer-Profile, Tester-Profile	192.168.43.6	AWS-UW2-SAML-VPN-GW-1	2020-04-05 08:29:02	73.93.180.214
mike@abc.com	invalid_saml_profile_ Default-Deny-	192.168.43.10	AWS-UW2-SAML-VPN-GW-1	2020-04-05 08:28:28	73.93.180.214

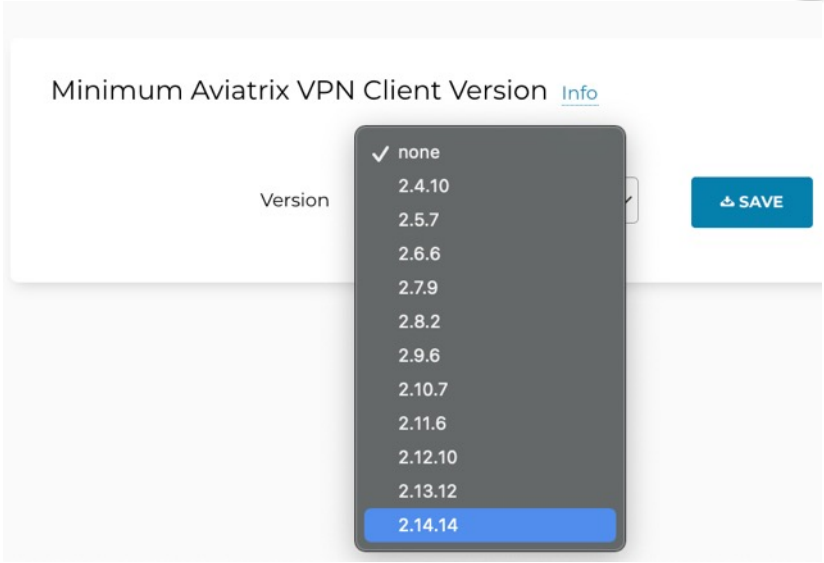
Preserve Client IP

- 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



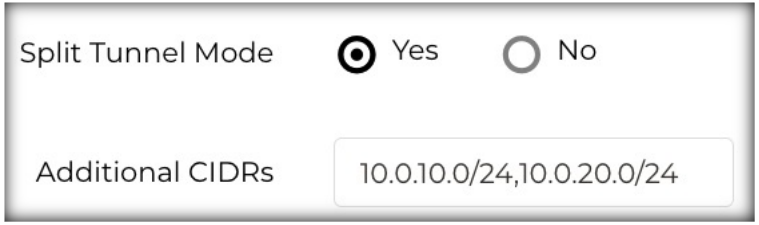
Minimum Client Version & Duplicate Connections

- 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



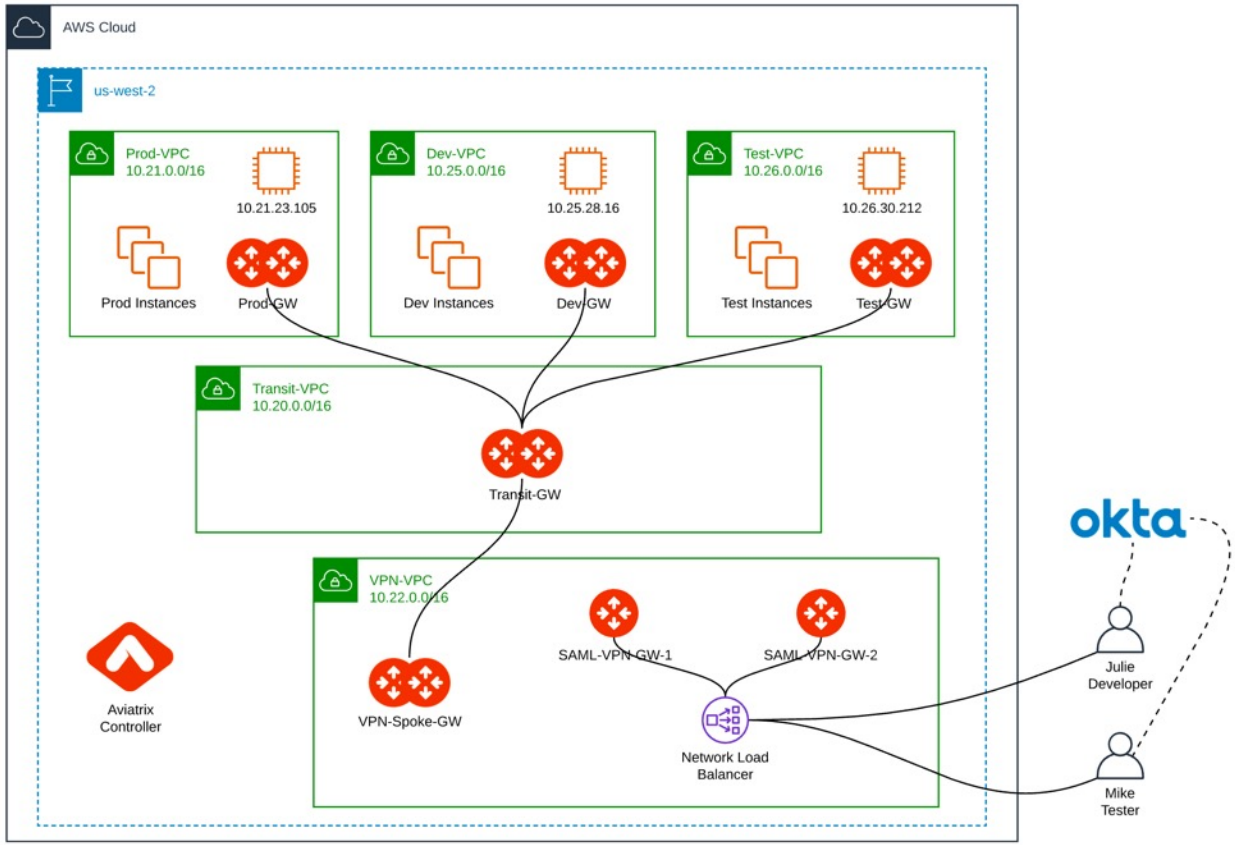

```
[umair@umair-mbp ~ % ifconfig utun5
utun5: flags=8051<UP,POINTOPOINT,RUNNING,MULTICAST> mtu 1500
        inet 192.168.44.6 --> 192.168.44.5 netmask 0xffffffff
[umair@umair-mbp ~ % netstat -r
Routing tables

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

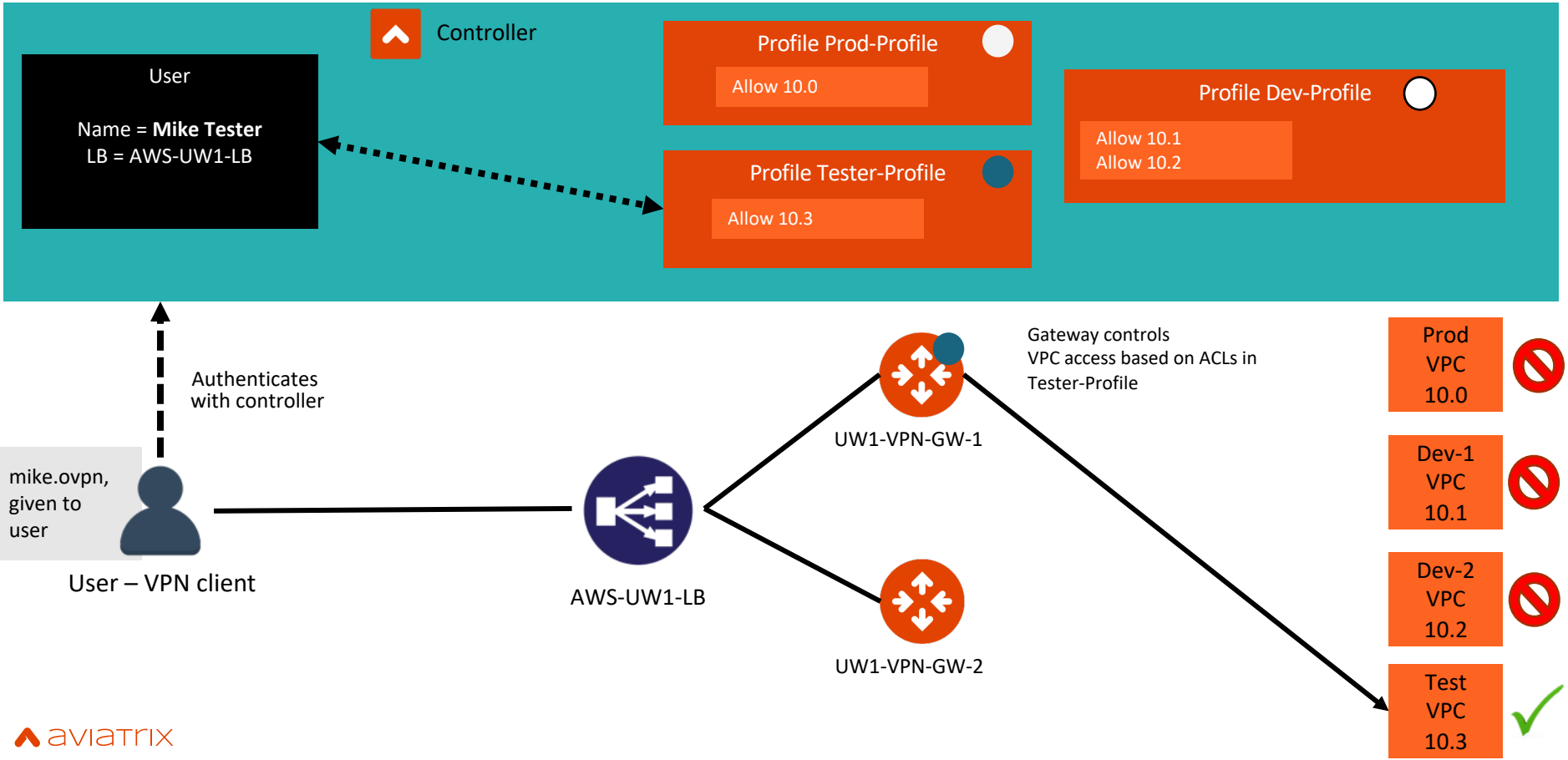
- Users will automatically get reconnected to another VPN gateway behind the load-balancer
- No change of certificate or user intervention

```
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 ~ %
```

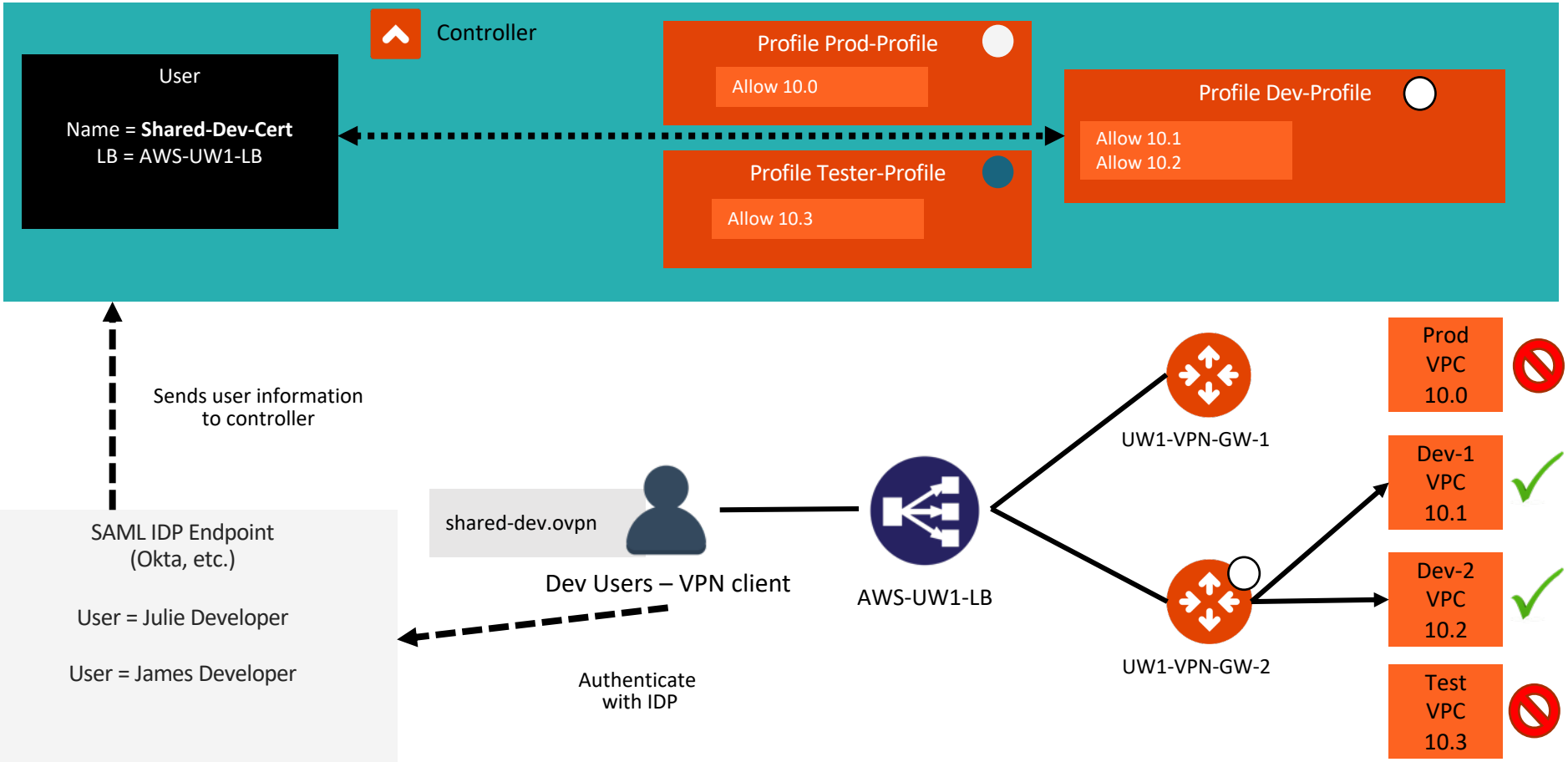
UserVPN Reference Architecture



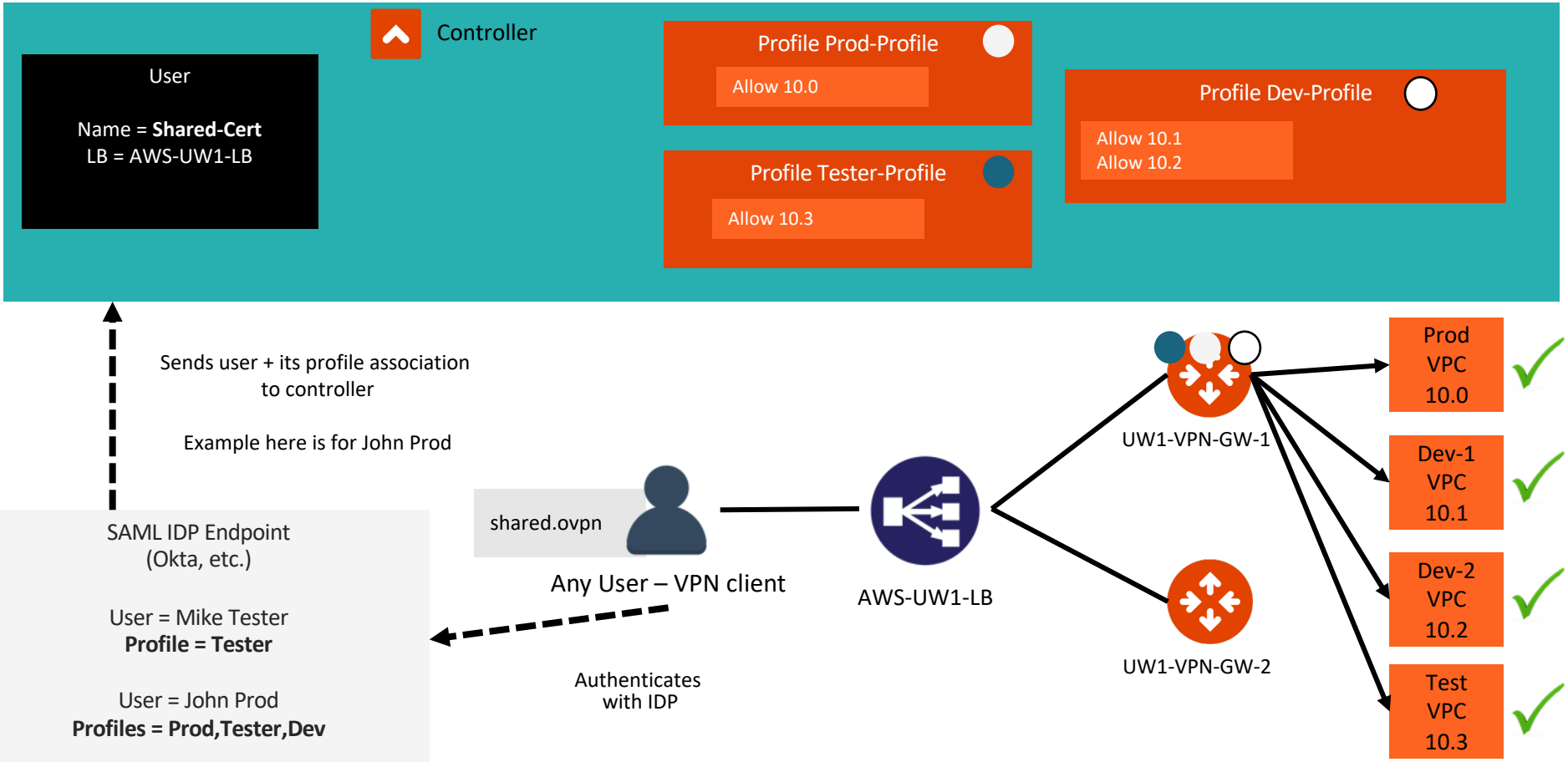
Users and Profiles



Users in IDP, Profile Association in Controller



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



Architecture Guidelines

Key Elements to Consider

- Performance Numbers - https://docs.aviatrix.com/HowTos/openvpn_design_considerations.html#simultaneous-clients-on-a-given-vpn-gateway
- (VPN gateway throughput) / (throughput requirement per client) = number of clients per gateway
  - Take into account the client-to-VPN gateway latency, and client type (Windows vs. Linux)
  - Example:
    - 100 ms latency → 200 Mbps VPN gateway with Windows clients
    - Requirement of 10 Mbps max burst per client → 20 clients per VPN gateway
- Region
  - LBs and VPN gateways are regional constructs
  - User location determines which LB they will connect to
  - Geo VPN or not?

Key Elements to Consider (cont.)

- Split-tunnel vs. full-tunnel.
  - Currently defined on a per LB/GW basis.
- Max number of connections per LB/VPN gateway is very high, so it's typically not a limiting factor.
  - For reference, AWS LB can handle 50K connections, Aviatrix VPN gateway can handle 64K connections.
- Max number of targets between a LB is not typically a limiting factor.
  - For reference, AWS LB can handle 1000 targets.

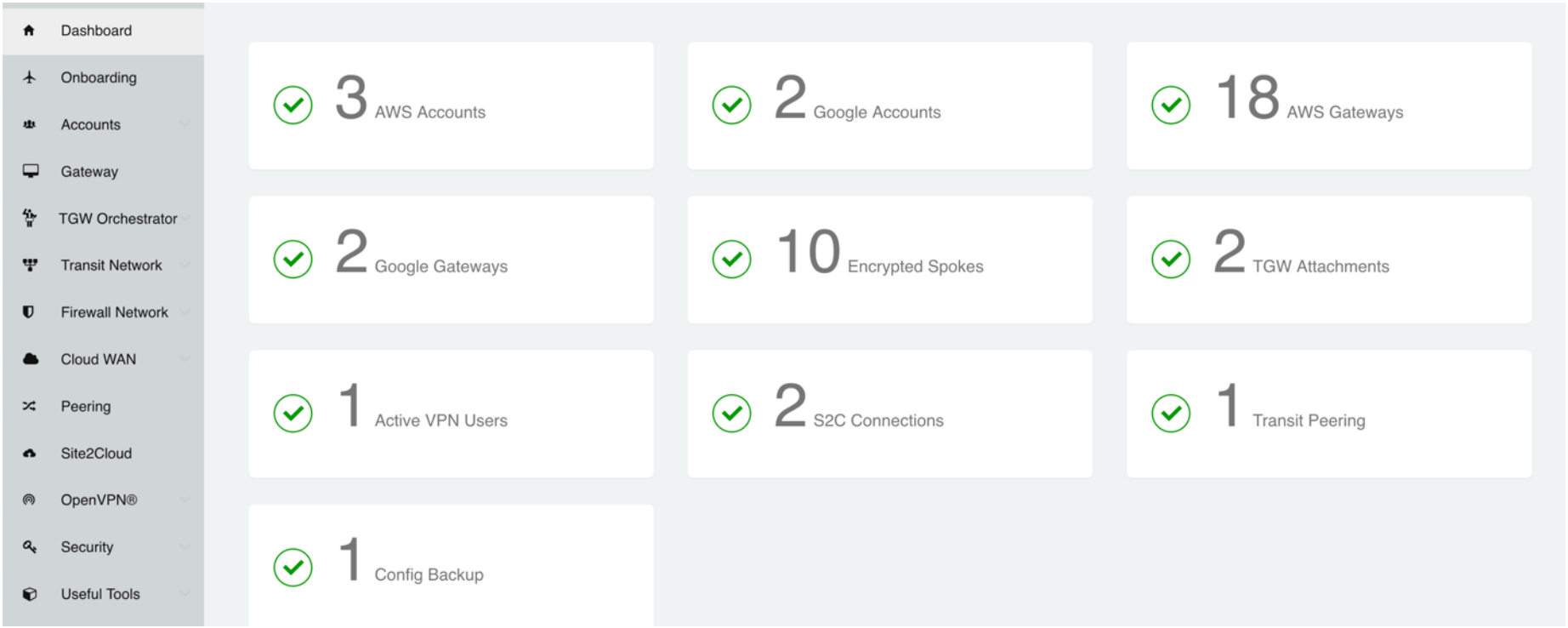
Best Practices

- Separate VPN functionality from other functionalities (Spoke, Transit, Egress FQDN, …)
- Separate VPC/VNet for VPN.
  - VPN gateway ←→ Spoke gateway traffic is routed in the VPC underlay.

Visibility and Troubleshooting

Reference

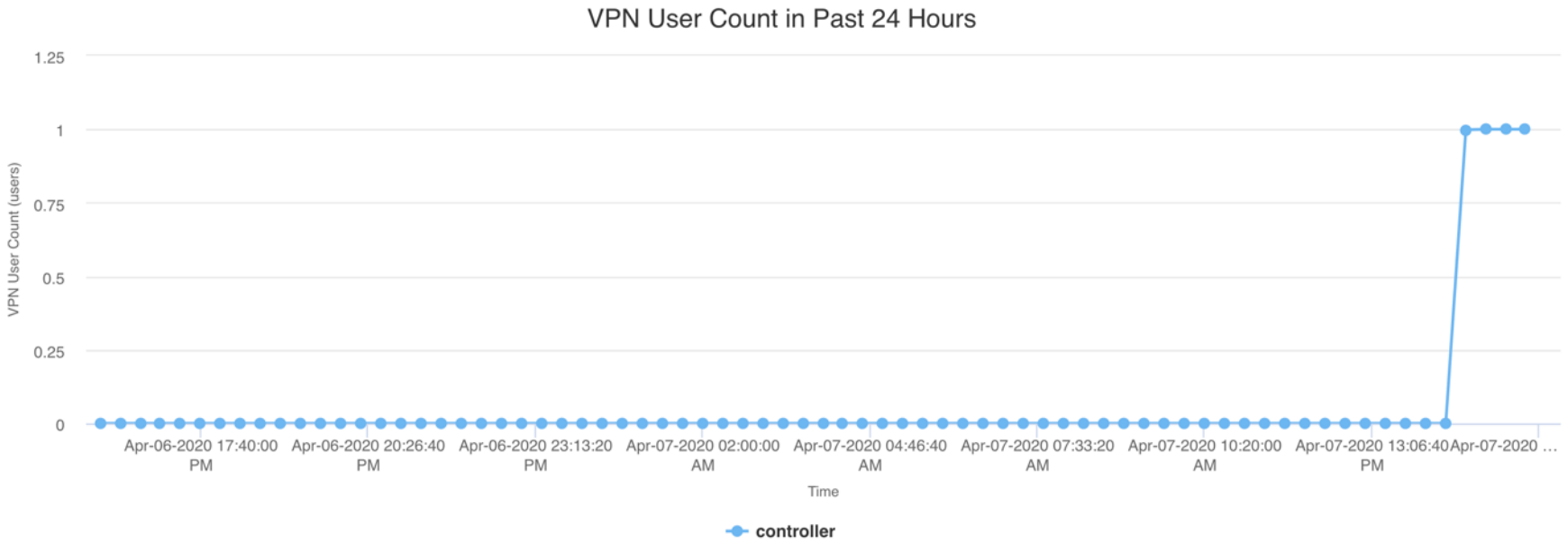
Visibility and Troubleshooting



Visibility and Troubleshooting

VPN USER COUNT

Time range Past 24 Hours



Visibility and Troubleshooting

ACTIVE VPN USERS TOTAL: 1

Search history

Name	Profile	Virtual IP	Landing Gateway	Login Time	Public IP	Platform	GUI Version	Actions
julie@abc.com	Developer-Profile, Tester-Profile	192.168.44.6	AWS-UW2-SAML-VPN-GW-2	2020-04-07 14:40:15	73.93.180.214	mac	AVPNC-2.7.9	Disconnect View

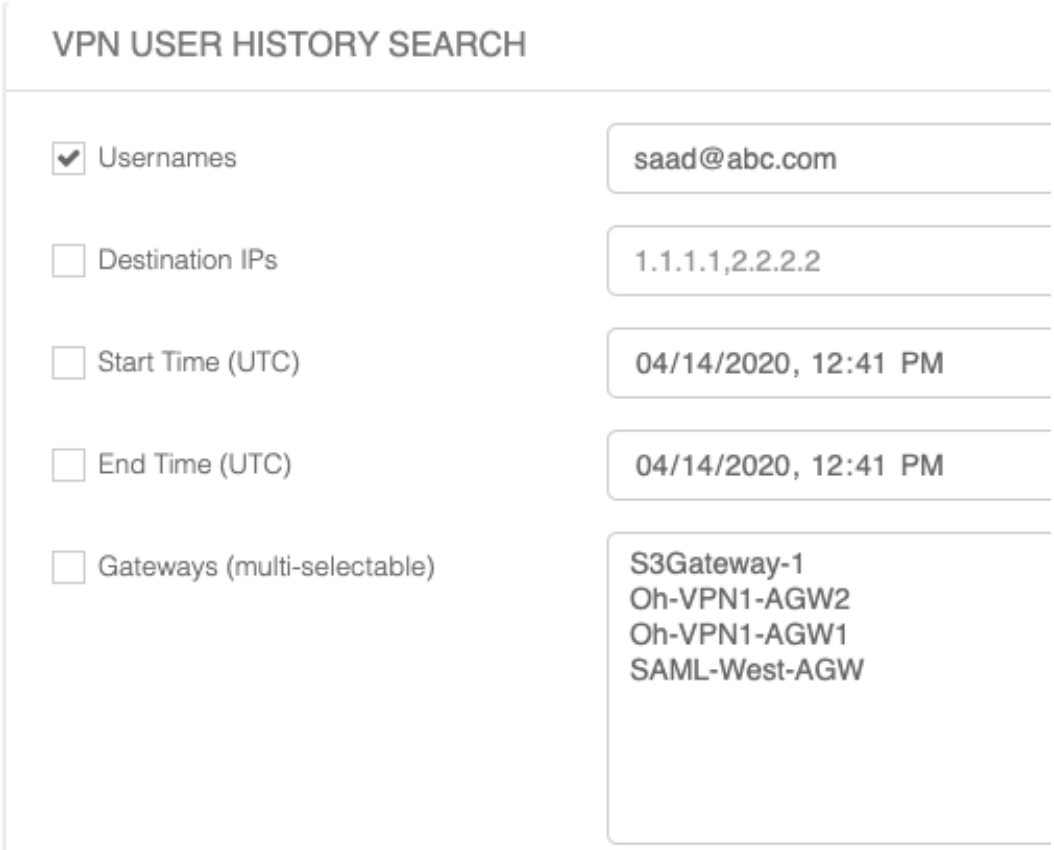
VPN session history

julie@abc.com

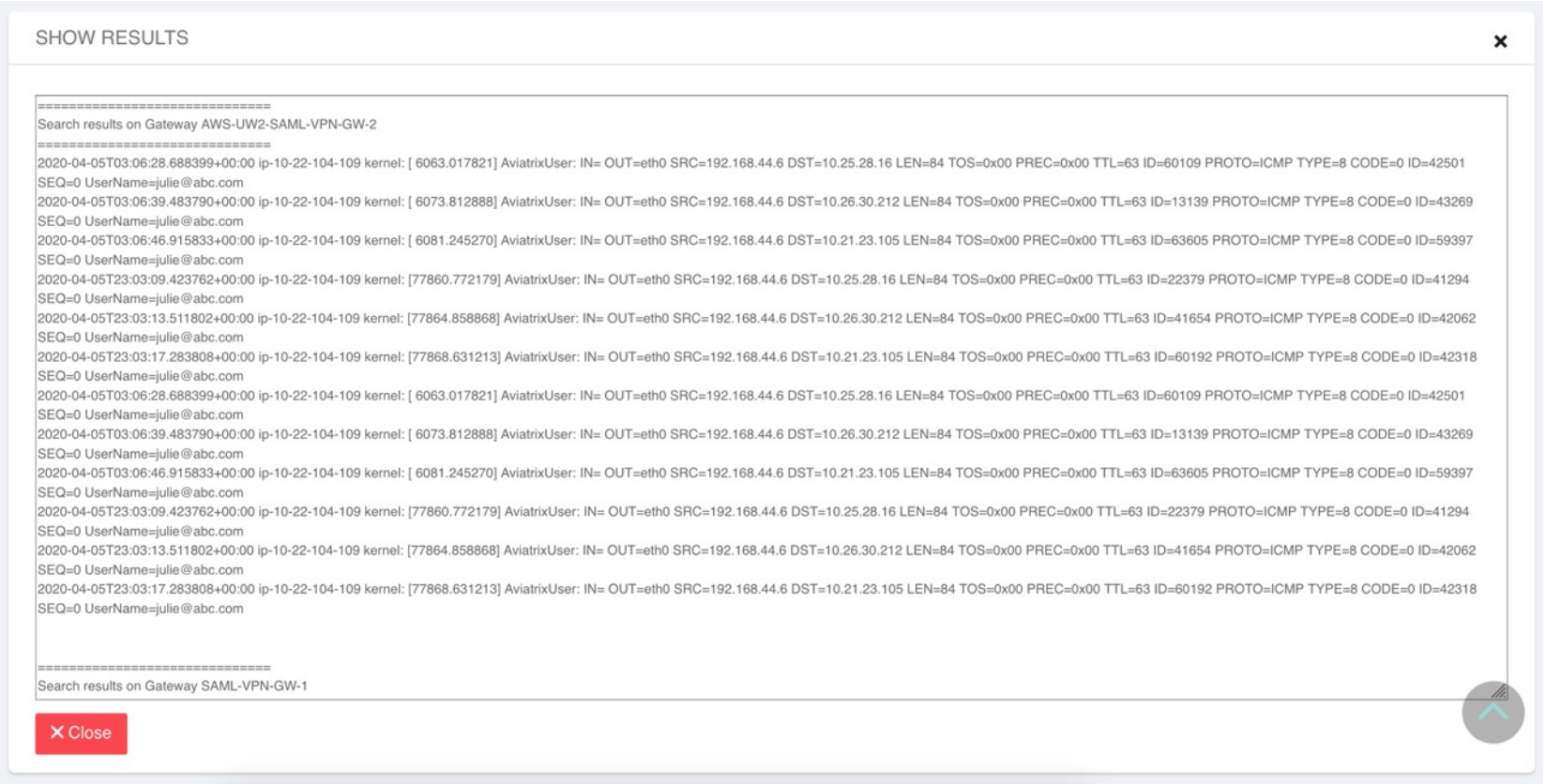
Go

Profile	Remote IP Address	Login Time	Logout Time	Session Duration	Gateway Name	Public IP	Bytes transmitted
Developer-Profile, Tester-Profile	192.168.44.6	2020-04-07 16:18:34	N/A	N/A	AWS-UW2-SAML-VPN-GW-2	73.93.180.214	N/A
Developer-Profile, Tester-Profile	192.168.43.6	2020-04-07 15:58:20	2020-04-07 16:12:33	0:0:14:13	SAML-VPN-GW-1	73.93.180.214	7.65KB
Developer-Profile, Tester-Profile	192.168.44.6	2020-04-07 15:31:12	2020-04-07 15:50:01	0:0:18:49	AWS-UW2-SAML-VPN-GW-2	73.93.180.214	8.8KB
Developer-Profile, Tester-Profile	192.168.44.6	2020-04-07 15:28:41	2020-04-07 15:31:15	0:0:2:34	AWS-UW2-SAML-VPN-GW-2	107.199.62.57	5.01KB

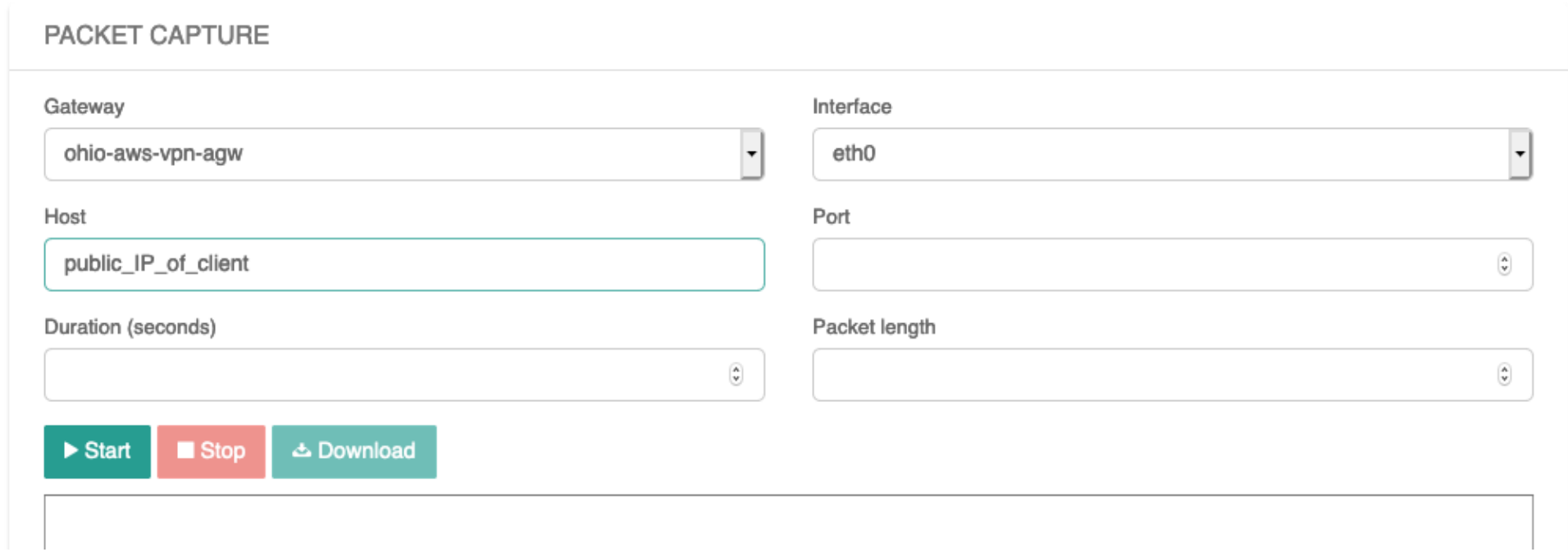
Visibility and Troubleshooting



Visibility and Troubleshooting



Take Packet Capture for Troubleshooting




aviatrix
ACE
Aviatrix Certified
Engineer