



Least Privilege Access

ACE-Security

Least Privilege Access

Tenet from NIST Publication 800-207 - Zero Trust Architecture (ZTA)

Trust in the requester is evaluated before the access is granted. Access should also be granted with the least privileges needed to complete the task.

- Trust no one, not even internal services, resources, and actors
- User VPN
- RBAC
- Parameter security solutions not sufficient (lateral movement)

RBAC

Aviatrix RBAC Control

The screenshot displays the Aviatrix CoPilot interface. On the left is a dark sidebar with navigation options: CoPilot, SmartGroups, Cloud Resources, Monitor, Diagnostics, Billing & Cost, and Administration. The 'Administration' section is expanded, showing 'User Access' and 'Reports'. The main content area has tabs for 'User Access', 'Users', 'Permission Group' (which is active), and 'Access Management'. Below the tabs is a '+ Permission Group' button and icons for filter, table view, and download. A table lists the configured permission groups.

Name	Copilot Visibility	Controller Permissions
admin	All	Write
read_only	All	Read
copilot_permission	All	Write
security	All	Security - Write
operations	All	Dashboard - Write
networking	All	Write
Aviatrix Demo Contro...	All	Write

Authentication

Users can be authenticated **Locally** or using **SAML IDP**.

The screenshot displays the AviaTrix Access Management interface. On the left is a dark sidebar with a search bar and a menu containing: Networking, Security, SmartGroups, Cloud Resources, Monitor, Diagnostics, Billing & Cost, Administration, User Access (highlighted), and Reports. The main content area has tabs for User Access, Users, Permission Group, and Access Management. Under the Access Management tab, there's a 'history' section with a 'Manage Policy' button. Below that is the 'Login Authentication' section, which includes a 'SAML' subsection. In the SAML section, there's a '+ SAML Endpoint' button and a search bar. A table lists the configured SAML endpoints:

Name	Permission Group	Access Set By	Test
aviatrix_saml_sso	profile_attribute	https://172.64.1.114/flask/saml/login/aviatrix_	[Edit] [Delete] [More]



onelogin

okta



G Suite

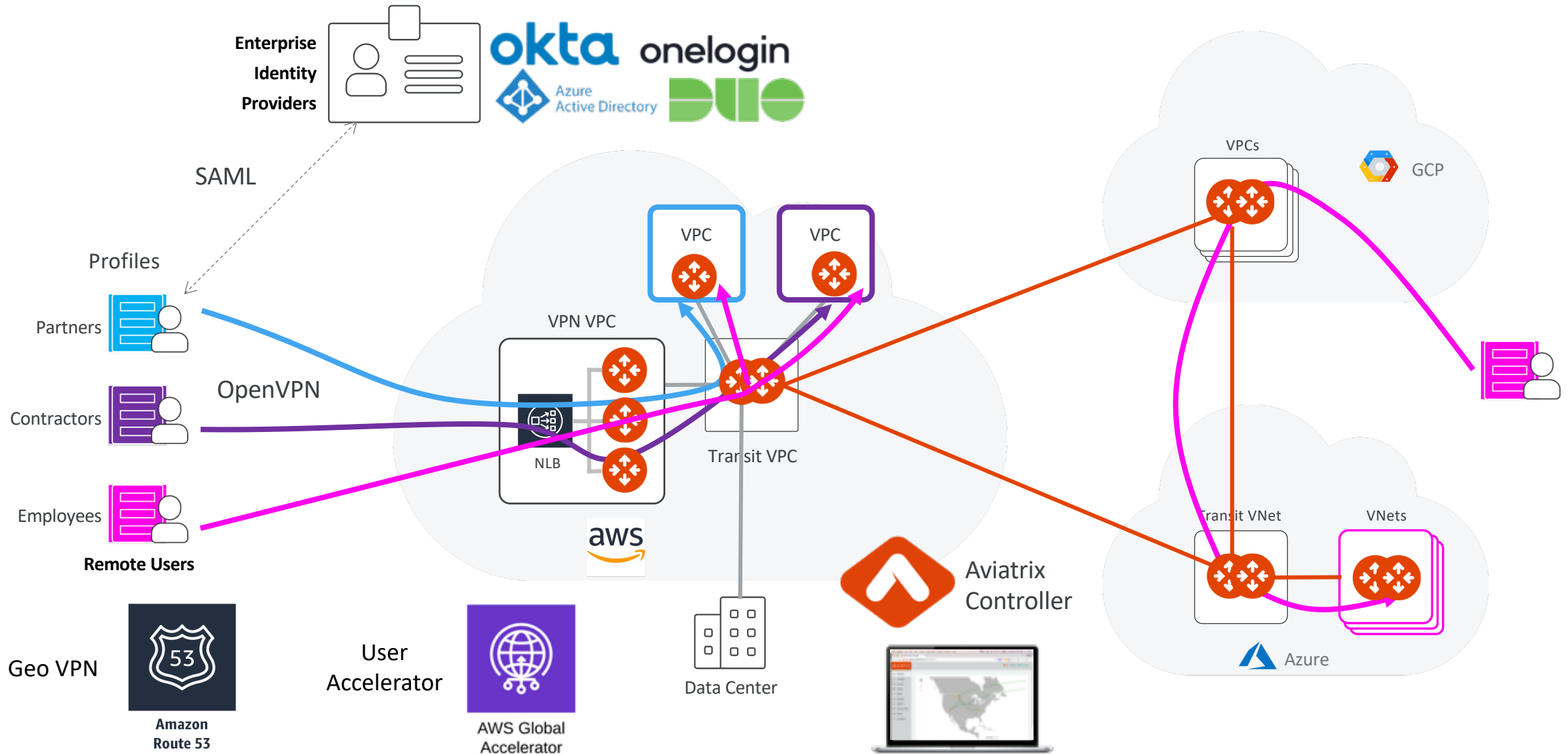


AWS SSO



Aviatrix User VPN

Least Privilege Access for Developer – Aviatrix User VPN





Aviatrix Certified Engineer (ACE)

<https://aviatrix.com/ACE>



COMMUNITY

<https://community.aviatrix.com>