

Next-Gen VPN solution for Sinorbis

By: AHEAD OF THE CURVE PTY LTD

 Scope (AWS)	1
 Research insights	1
 Design options	2
 Follow up Steps	4
 Terms and Conditions	4

? Scope (AWS)

- Establish a VPN connection service/server that controls the network connection to the private VPC networks in the Sinorbis AWS cloud account (Sydney/HK regions). Each VPN connection will control access to one VPC network in the Sinorbis AWS account. There are 2 VPC networks in the Sydney and HK region (including QA and production).
- Implement an access control mechanism in the established VPN connections, so that only authenticated users can use the VPN connection. Each user should have their own credentials when accessing/using the VPN connection. E.g. public/private key auth. User credential management should be secure and friendly to allow the easy creation and removal of users.
- The following criteria needs to be delivered in the VPN connection: secure, auditable, traceable, scalable



Research insights

As discussed in the last meeting, Sinorbis needs several solutions to be chosen for their new VPN connections. The existing solution with OpenVPN Community is out-of-date and hard to maintain

Since the network is built on AWS Cloud, one solution is to use the AWS managed service, called "AWS Client VPN"

The OpenVPN Access Server (Enterprise version), OpenVPN Cloud and AWS Client VPN solutions are compared below:

Design options

Features	<u>Option 1</u> AWS Client VPN	<u>Option 2</u> OpenVPN Access Server (Enterprise)	<u>Option 3</u> OpenVPN Cloud
Consultant fee	\$2000 + 10%GST, includes <ul style="list-style-type: none"> Understand the project (Done) Workshop to go discuss the solutions (This fee can be waived if you choose our company to run the implementation)		
Environment	2 VPC networks in the Sydney and HK region (including QA and production).		
implement fee	\$5000 ~ \$10,000 + %10GST Depends on extra features, such as AD integration, multi-region AD connector support, automation deployment and others	\$5000 ~ \$10,000 + 10%GST Depends on extra features, such as AD integration, redundant & Cluster, AD connector support, automation deployment and others	\$3000 ~ \$5000 + 10%GST Depends on extra features, such as AD integration, automation deployment and others
Unit price per day	\$1000 + 10%GST per day	\$1000 + 10%GST per day	\$1000 + 10%GST per day
Estimated days	5 ~ 10 days	5 ~ 10 days	3 ~ 5 days
Recommendation	✓✓	✓✓✓	✓✓✓✓
Features			
Managed service (VPN-as-a-Service)	Yes	No	Yes
Same solution is suitable for Alibaba Cloud	No	Yes	Yes
TLS encrypted VPN tunnels	Yes	Yes	Yes

Features	<u>Option 1</u> AWS Client VPN	<u>Option 2</u> OpenVPN Access Server (Enterprise)	<u>Option 3</u> OpenVPN Cloud
Client software	Yes (AWS VPN Client)	Yes (OpenVPN Connect)	Yes (OpenVPN Connect)
Build VPN Server	No Managed Service	Yes management of the vpn server is necessary	No but need to deploy OpenVPN connector to each VPC
Access Control	<ul style="list-style-type: none"> With user-based authentication, you can grant specific groups of users access to specific parts of your network. Not for mutual authentication 	If you enable group access control, you can permit group access to specific subnets and services.	An Access Group can limit access from a set of one or more Hosts, Networks, and User Groups to another set of one or more User Groups, Services, Hosts, and Networks.
MFA enable with user account	Yes need enable with AD	Yes	Yes
Auditable & traceable	Yes	Yes	Yes Error logs for the last 24 hours are visible in the Administration Portal
Scalable	Yes Managed service	Yes but more effort. Multiple Access Server deployments are needed for redundancy. Clustering provides for active/active redundancy for fault-tolerant deployments.	Yes Managed service
High-availability failover solution	Yes Managed service	Yes need extra effort to set up	Yes Managed service

Next-Gen VPN



Features	<u>Option 1</u> AWS Client VPN	<u>Option 2</u> OpenVPN Access Server (Enterprise)	<u>Option 3</u> OpenVPN Cloud
Multi-region support	with Microsoft Active Directory (AD) and Amazon Route 53	Multiple VPN servers that are located in each Region	Install Connector in each VPC
Built-in Authentication	Certs/AD/SSO	PAM/LDAP/RADIUS/AD/local user database	- Users are authenticated using OpenVPN Cloud Directory / SAML/Single Sign-On (SSO)
Centralized management	No	No	Yes, with OpenVPN Cloud Directory Firewalls don't need to be opened to allow incoming traffic from the internet.
Backup	No Managed service	Yes	No Managed service
Maintenance	Low Managed Service	Medium Keep VPN server update to date	Low Managed service, but still need manage connectors
Cost			
Basic Operating expenses for 10 users includes licenses	\$228 per month +10%GST See attached	\$75 per month (get 20% discount on licenses if pay annually)	\$75 per month (get 20% discount on licenses if pay annually)
(Optional) AWS Directory Service (AD)	Around \$288 per month	Around \$288 per month	Not required
Server hardware cost	No	Yes Around \$20 for a t3.small instance (openvpn server)	Yes Around \$20 for a t3.small instance (openvpn connector)

Follow up Steps

- Decide upon an appropriate solution
- 50% consultant & implement fee is to be paid in advance
- Implement the solution in one to two weeks, depends on the complexity
- Remaining fee is to be paid
- 1 month BAU support within 5 hours (includes in implement fee)

Terms and Conditions

1. The consulting services for implementation are provided on a time and materials (T&M) basis; that is, you shall pay for time incurred performing the services, plus materials, taxes and expenses.

2. The implementation fee estimate is provided by Ahead Of The Curve Pty Ltd from the knowledge gained from communications with customer Sinorbis Holdings pty Limited. Ahead Of The Curve Pty Ltd will take all reasonable care to ensure that the services provided are performed

within the estimate provided. However unforeseen complexities do arise that may exceed the contingencies allowed for and the time taken may exceed the estimate. This time is chargeable. Conversely if the project is completely finished and closed in less time than the estimate, then the unused time will not be charged for. Where it becomes possible that the estimate will be exceeded, Ahead Of The Curve Pty Ltd will discuss this with the customer's project manager to determine the new extended estimate, and whether that or other functionality can be simplified or reduced in scope.

3. Any responsibilities of the customer that are not met in time or in function will cause a review of the implementation fee estimate and/or may incur a charge for waiting time. Such a delay is also likely to require a delay to remaining schedule milestones and a re-booking of Ahead Of The Curve Pty Ltd resources for a later date when they are next available.

4. A written Change Request needs to be raised and approved by both parties for any agreed changes to the deliverables, consulting services or other material aspect of this proposal.

5. The price excludes consultant Travel and Disbursements. Travel and Disbursements are chargeable in addition to the price for consulting services.

6. Any commitment Ahead Of The Curve Pty Ltd makes to deliver on a certain date can be adjusted at our discretion if the customer changes requirements or causes delays to the project.

7. All prices are in Australian dollars and exclude GST

8. This proposal and the work to be undertaken is subject to the terms and conditions of the Software and Services agreement between the customer and Ahead Of The Curve Pty Ltd which is required to be signed prior to delivery or installation of the software and

Next-Gen VPN



commencement of the implementation project.

9. All information provided by Ahead Of The Curve Pty Ltd in this Proposal is to be treated as Confidential Information and is provided solely for the purpose of enabling customer to evaluate Ahead Of The Curve Pty Ltd Proposal.

10. If you have any queries or concerns with these conditions, please contact Ahead Of The Curve Pty Ltd before signing the agreement to have the work performed.

Ahead Guru