# Cloud Security Crucibles: Australia and New Zealand

**David Holmes, 2016-09-05**

I've just returned from a long tour of Australia and New Zealand (ANZ), where some exciting developments are worth capturing. Both countries are island nations, and one thing Darwin noted in "On the Origin of Species" is that islands can become crucibles of evolution. Australia is evolving a new way to leverage cloud, and New Zealand is evolving a new efficiency model for government security services. Both countries share one aspect with the rest of the world: challenges around encryption.

## Australia is evolving multi-cloud

For the last five years, no one has embraced cloud more fully than the Australians. The financial services industry is usually the last to the Cloud party in most regions, but not in Australia. Down Under, the financial services industry has been leading the way with cloud-first policies. Now the Australians are aggressively pursuing the multi-cloud strategy as well.Multi-cloud employs multiple public clouds; AWS, Google, and Azure are among the three largest. It has advantages over a simple cloud-first policy, but security isn't one of them.

Australians see two main benefits of adopting multi-cloud architecture. Adaptive utility cost is the first. Different cloud providers charge different rates, and these can vary day to day, or even hour to hour. An agile architecture can take advantage of these price differences by shifting compute and storage loads to the current cheapest compute and storage providers.

Second, the Ozzies are keen to avoid a single point of failure; just because cloud is "someone else's computer" doesn't mean it is somehow magically immune to operational error. For example, Microsoft's Azure public cloud suffered a global failure when one of its SSL certificates expired unnoticed. Customers using only Azure during the outage would have been left high and dry. But those with a multi-cloud strategy, in theory, would see their business processes increase production in the other two public clouds to compensate.

One Australian customer wants to build an application with five components, each of which can be in a different public cloud at any time. The components can shift from public cloud to public cloud to take advantage of utility pricing or to avoid outage.

The difficulty here lies in securing the application components when they're shifting from cloud to cloud. Any traffic traversing from one public cloud to another is by definition crossing the Internet and should therefore not be trusted. Each component must treat each of the others as untrusted.

The nascent cloud access security broker (CASB) industry is trying to take on this problem by wrapping each component in its own tunnel and providing layer 2 tunnels to each. This is an interesting approach, but the fact that the CASB provider has to build a virtual cloud among the public cloud reintroduces the single point of failure: the CASB provider itself.

Multi-cloud security is a difficult problem to solve--one that the Australians are graciously tackling before the rest of the world has to.

## New Zealand is evolving Telecom-as-a-Service (TaaS)

Managed service providers and resellers in New Zealand are banding together to form a TaaS consortium. TaaS is a new concept in selling both kit and maintenance specifically to sovereign government agencies. With TaaS, the buyer chooses the components (and vendors) of a technical solution, but rents them instead of owning them. The managed service provider also runs the management and operations of the solution.

The driver for TaaS is a change in the way the New Zealand government is allocating funds: capital expenditure is almost impossible to get approved, where operating expenses get approved quite easily. Therefore government agencies are moving toward the TaaS model, where they don't own the kit or manage the services but still get to choose the solutions. This hasn't been tried anywhere else in the world (that I know of), so we'll be keen to see how it works out. The billing model sounds complicated. The consortium is preparing to launch the TaaS model in Australia as well.

## Encrypting Down Under

Even though both countries are pioneering these new frontiers, they do have something in common with the rest of the world: challenges around encryption and security. Nearly every organization I visited was excited about F5's new SSL Recommended Practices (SSL RP). Released late last year, the SSL RP provides a detailed, exhaustive guide for dealing with the encryption challenges that so many organizations are facing as they work to "encrypt everything."

The SSL Recommended Practices topics include:

- How to get an A+ from Qualys SSL Labs.
- Four ways to perform certificate revocation.
- Three ways to mirror SSL data for high availability.
- Configuring F5 as a forward proxy to support SSL inspection.
- When should an organization use Forward Secrecy?
- Boosting security posture with Strict Transport Security.

The PDF of the SSL Recommended Practices can be downloaded from the F5.com site.

## Thanks to the crucial crucibles

The island nations of Australia and New Zealand can be evolutionary crucibles for new technologies. If TaaS succeeds in New Zealand and migrates to Australia, it might grow enough to spread to the rest of the world. Ironing out the wrinkles in the multi-cloud fabric may take longer than the development of TaaS. But if the Australians figure out how to smooth multi-cloud, it's easy to see the entire developed world moving toward it for the betterment of services everywhere. It will take some time, though.

F5 Networks, Inc. | 401 Elliot Avenue West, Seattle, WA 98119 | 888-882-4447 | wwww.f5.com

F5 Networks, Inc.
Corporate Headquarters
info@f5.com

F5 Networks
Asia-Pacific
apacinfo@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com