CASE STUDY

Building Security and High Availability for Complex, Cloud-based Geospatial Analysis

AmigoCloud delivers a big data platform and associated services that enable organizations to collect geographic information system (GIS) data in the field, upload the information securely to the cloud, and analyze it along with other proprietary and publicly available datasets to solve highly complex geospatial problems. Founded by a team of GIS experts in 2013, AmigoCloud is headquartered in San Francisco and has a branch office in Lima, Peru.

AmigoCloud's client list is diverse, and includes investment firms wanting to identify the real estate properties most likely to be profitable, utilities needing to streamline services to customers, and transportation departments that must track everything from potholes to street signs. The company serves several U.S. government agencies as well, which impose highly specific security requirements and demand frequent compliance certifications.

"In general, GIS data is not very sensitive, as things like road networks and street signs are not private information," explains Daniel Caldwell, director of engineering for AmigoCloud. "But that changes significantly when we do work related to the national electrical grid. And it changes in a big way when it comes to intelligence activities."

Cloud-first from Day One

AmigoCloud has utilized a cloud-based architecture from the beginning, in an effort to deliver the flexibility, scalability, and total cost of ownership (TCO) required to profitably deliver its wide range of services. "Our customers' needs are very diverse, so we require an agile and flexible infrastructure to deliver to their specifications," says Caldwell.

"We use our in-house data center for testing and some production projects, but most of our data analysis work takes place in the cloud," Caldwell continues. "We started by leveraging public clouds, ultimately settling on Amazon Web Services (AWS)—and its GovCloud offering for government customers. But because of customer requirements, we now also have a private cloud infrastructure that we built five years ago, and much of our newer work is being housed there."

"FortiGate gives us transparent visibility across our entire hybrid architecture, both the on-premises data center and the AWS cloud."

– Daniel Caldwell, Director of Engineering, AmigoCloud

Details

Customer: AmigoCloud

Industry: Technology

Location: San Francisco, California, USA

Deployment

- FortiGate
- FortiSwitch
- FortiGate Unified Threat Management Bundle
- 24×7 FortiCare Support

Struggling with Piecemeal Security

When AmigoCloud built out its initial solution offerings, Caldwell elected to use an open-source firewall and router to protect the data center. But a few years in, their experience with that solution was less than positive. For one thing, because of consumer-grade components in place at the time, they could only use one of the data center's two connections, essentially cutting throughput in half.

In addition, the system had inadequate failover capabilities, which compromised availability and reliability and made it difficult to perform even scheduled maintenance. "Installing an infrastructure upgrade could bring down the whole system," says Caldwell. "It got to be an unacceptable level of risk."

The open-source firewall also posed problems for troubleshooting. "The worst part was the lack of visibility," Caldwell says. "When an application began to have poor response times, my team might have a sense of where the problem was located, but they couldn't pin it down. The tools were inadequate. As a result, it was impossible to know what was truly happening in our network."

Meeting Strict Security Requirements for U.S. Agencies

An opportunity to address these problems began a year ago, when a U.S. agency asked for proposals to build a geospatial analysis platform for highly sensitive intelligence projects. AmigoCloud would not host this analysis at all; the customer wanted to do all the data analysis on-premises using dedicated hardware, with limited and secure connectivity even within its own data center.

After a rigorous procurement process, the agency awarded the contract to AmigoCloud, which included providing the dedicated hardware infrastructure and an instance of AmigoPlatform. The latter can analyze datasets up to petabyte scale and display the results in a customizable graphical format.

Above all, the agency needed to avoid interruptions to its critical intelligence workflows. "High availability was a crucial requirement for both the hardware and the software," says Caldwell. "If an outage lasts longer than 48 hours, the agency can impose a big fine on AmigoCloud, which would be a highly embarrassing incident for both parties." Because of the sensitive nature of the data, the AmigoCloud network had to be physically separate from other networks in the agency.

Turning to a Trusted Advisor

"Regarding security, our first big decision was, 'Should we do it ourselves using the open-source firewall or outsource the project to a cybersecurity vendor?'" Caldwell says. "Given our experience, we were not confident that our incumbent firewall could do the job." AmigoCloud had an existing relationship with Fortinet, so Caldwell and his team approached that company to jointly design security into the dedicated hardware platform from the ground up.

AmigoCloud opted for two FortiGate next-generation firewalls (NGFWs) configured in high-availability (HA) mode. "We chose FortiGate in part because of its ability to provide visibility and management control across a container-based environment," says Caldwell. "It also met our client's requirements for high availability."

Business Impact

- 15 hours in staff time per month saved due to dynamic DNS configuration
- 15 hours in staff time per month saved due to more efficient alert handling
- Thousands of dollars in avoided capital spending using a GPU subsystem
- Able to meet 48-hour SLA mandated by government agencies
- Improved availability from 98.90% to 99.99%

"The FortiGate NGFWs save me five hours every time we set up a dynamic DNS for our clients."

– Daniel Caldwell, Director of Engineering, AmigoCloud

"Our meticulous preparation paid off, because the installation went without a hitch."

– Marco Flores, Professional Services Tech Lead, AmigoCloud

The company chose the FortiGate Unified Threat Protection (UTM) bundle to extend protection to web- and email-based attacks. The architecture also includes two FortiSwitch secure access switches that are cross-connected to the servers for redundancy.

AmigoPlatform is a cloud-native application based on containers with Kubernetes orchestration. In case of a component failure, the Kubernetes cluster reallocates hardware resources to ensure continued service availability. FortiGate NGFWs are container-aware, automatically updating dynamic addresses for Kubernetes and providing a high level of visibility and control across the end-to-end environment.

> *"The response times that we get from Fortinet are phenomenal—not like other vendors who make you wait 48 hours to get a real response."*
>
> – *Daniel Caldwell, Director of Engineering, AmigoCloud*

Deployment with No Outside Resources

The agency's tight security imposed significant constraints on the installation team. "Once you go inside the facility, you are not allowed to communicate with the outside world: no phone calls, no texts, no emails, no Google searches," explains Marco Flores, professional services tech lead for AmigoCloud. "Therefore, we decided to prototype the complete setup in our lab, perform extensive testing to ensure proper operation, then document the process on paper so we could do it again at the customer's location."

Local engineers from the Fortinet team were called in to help with the prototyping phase. The Fortinet engineers worked side by side with AmigoCloud to set up the equipment, configure the Kubernetes clustering and the FortiGate HA mode, test failover times and other requirements, and—most importantly—carefully and thoroughly document every aspect of the installation. "With the help of the Fortinet team, we created a detailed notebook that showed every physical connection, every configuration setting, every part number—everything," Flores says. "Our meticulous preparation paid off, because the installation went without a hitch."

Supporting the Agency's Mission

After 24 months of production operations, the AmigoCloud system is doing its job for the intelligence agency. "Everything has been working great," says Caldwell. "The FortiGate devices are handling a lot of traffic without any problems."

The agency is particularly pleased with the ease of security management made possible by the tight integration of the FortiGate and FortiSwitch devices. "The agency's security team can manage port-level security and policy enforcement from the FortiGate GUI," Caldwell says. "There is no need to go directly to the switch. They don't have to worry about separate switch and firewall layers or failing to completely account for east-west traffic."

The AmigoCloud team relies on FortiCare 24×7 technical support to meet the agency's service-level agreement (SLA) for remediating outages. "The response times that we get from Fortinet are phenomenal—not like other vendors that make you wait 48 hours to get a real response," says Caldwell.

Upgrading the Hybrid Cloud

The agency deployment worked so well that AmigoCloud has decided to rearchitect its hybrid cloud environment using Fortinet products and services. Caldwell's team has developed a set of requirements for the upgrade based on what they learned during the agency deployment. "For one thing, we want the same level of high availability that the agency has achieved with the Fortinet HA configuration," says Caldwell.

However, AmigoCloud has additional requirements for its hybrid cloud that go beyond those of the agency. To provide gigabit Ethernet connectivity between servers, Caldwell's team plans to pair together its two connections to the company's co-location facility to increase throughput.

Scalability and flexibility are additional goals of the upgrade. "We want to avoid investing in hardware that we only need temporarily," Caldwell notes. For example, AmigoCloud often runs TensorFlow model analyses, which are compute-heavy workflows that require a GPU. "It would cost us thousands of dollars to replicate the GPU capabilities that AWS provides on a pay-as-you-go basis," he explains.

Saving Time and Improving Efficiency

While the internal upgrade process is ongoing, AmigoCloud is reaping benefits from the Fortinet devices already installed. “FortiGate gives us transparent visibility across our entire hybrid architecture—the on-premises data center and private cloud as well as the AWS cloud,” say Caldwell. “Just getting the alerts right saves me three hours every week.”

Thanks to the internal DNS capabilities of FortiGate, AmigoCloud has streamlined the process of delivering results to its customers via custom URLs—something that happens two or three times a month on average. “Our analyses drive critical decisions such as whether or not to buy a particular tract of land for mining operations,” Caldwell says. “With such a high-value product, we don’t want to give them a long, complicated link to see their results; instead, we set up a simplified URL using the customer’s own name.” In the past, Caldwell had to configure the switches manually, something that happened at least three times a month. “FortiGate saves me five hours every time we set up a dynamic DNS for our clients,” Caldwell observes.

For the initial project with the U.S. government agency, the centralized visibility provided by the FortiGate NGFWs is a key benefit. “Being able to have full visibility and control over each Kubernetes container fulfills a key need for this customer,” Caldwell relates.

Keeping Ahead of the Curve

To increase productivity and improve operational efficiency, AmigoCloud is actively working to automate manual processes across the board. Caldwell’s team is currently evaluating FortiAnalyzer to bolster the company’s ability to identify threats and automate log management.

“We installed FortiAnalyzer to test out its capabilities,” Caldwell relates. “As soon as it was live, we could identify the sources of unusual or suspicious traffic. When we saw a large amount of traffic coming from Peru, where we have an engineering office, we knew this wasn’t an issue. But if we see traffic influxes from China, for example, then we know that we need to pay attention. We are impressed with the level of analysis we can do.”

Caldwell expects AmigoCloud’s relationship with Fortinet to grow even more in the future. “The Fortinet team has been extremely helpful in our deployments so far, and the fact that everything is seamlessly integrated will make it easy to add protection,” Caldwell concludes.

September 27, 2019 2:03 PM

476487-0-0-EN

Macintosh HD:Users:mbunnell:Documents:Egnyte:Shared:CREATIVE SERVICES:Team:Michael-Bunnell:Case-Study:CS-AmigoCloud:cs-amigocloud