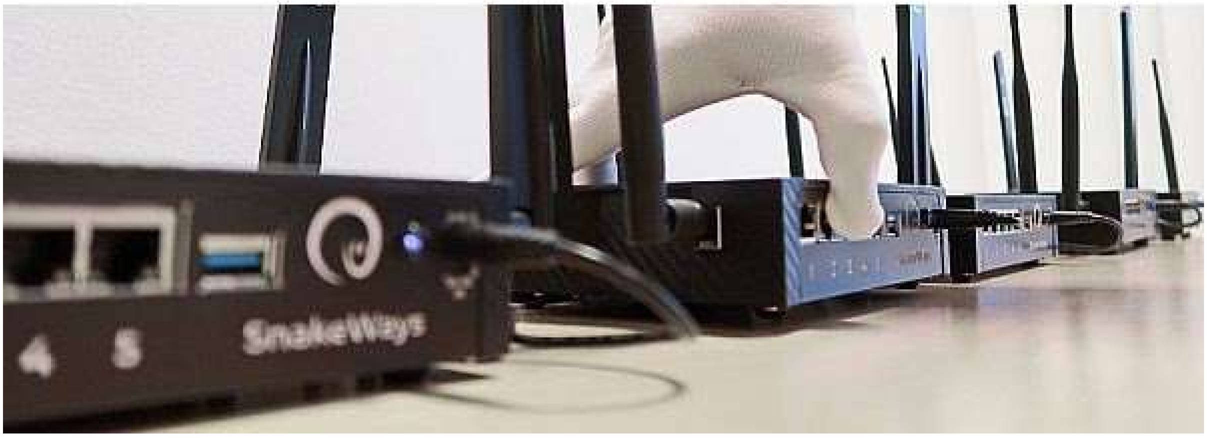
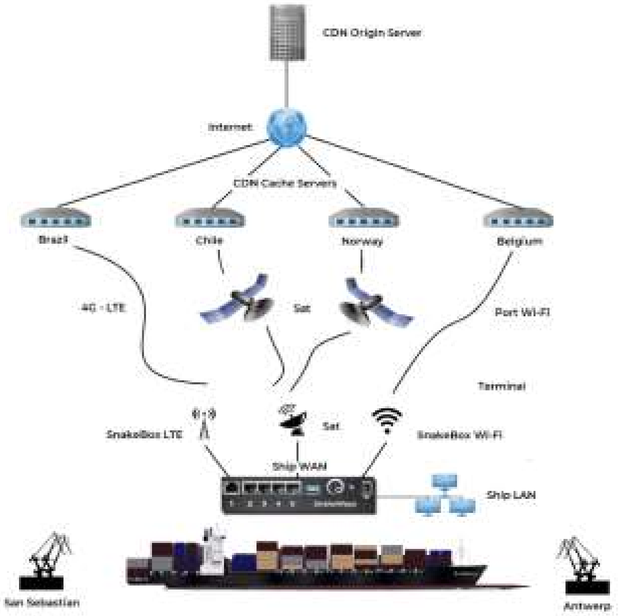
SnakeWays

Innovation Meets Experience



Does your shipboard firewall know about distributed content?

Many internet based services are now using distributed content delivery to improve performance. According to BuiltWith there are over 27 Million websites using a Content Delivery Network (CDN) to reach their subscribers and that includes a number of key maritime websites. Using a CDN provides undoubted benefits to a customer based in an office or at home with a stable connection to the internet. But what about the Tanker or the Container Ship trading across the world’s oceans using multiple mobile networks?

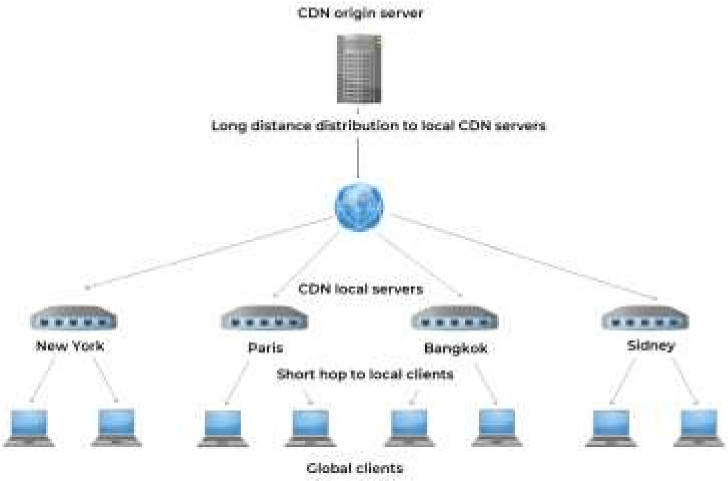


Firstly, what is a CDN, and how does it work?

A CDN is a network of servers that distributes content around the world from an “origin” server. It does this by caching that content on local servers close to where each end user is accessing the internet. An example would be a customer in Paris looking to book a room in Bangkok on Airbnb. Airbnb are headquartered in California, but the customer doesn’t need to connect to either California or Thailand. She simply connects to the local Paris server on Airbnb's CDN.

Now let's consider that Container Ship loading in San Sebastián (Brazil) for Antwerp (Belgium). She uses the UK Hydrographic Office for key safety and navigation updates downloaded over the internet. The UK HO uses a global CDN and whilst in San Sebastián the ship will connect to a local server in Vitoria over the Brazilian LTE/4G network. Similarly, on arrival at Antwerp she will connect to a UK HO content server in Brussels using a local LTE/4G service. But what about the ocean passage in between?

There are no CDN servers in the Atlantic, nor in space where the satellites are (not yet).



By default the vessel will connect to the CDN cache server nearest to where the satellite link comes back down to earth. That could be in any one of a number of ground stations strategically located in various countries around the globe. Almost certainly the vessel will use at least two different ground stations whilst on passage – one in the southern hemisphere, one in the north. Therefore, on one simple passage the vessel will make use of at least 4 different content servers in four different countries in order to keep the charts up to date.

Why does this matter? And why does your shipboard firewall need to know about it?

For the shipboard firewall, content such as SNMs provided via a CDN appear as a moving target, frequently shifting location on the internet. One day they are being delivered through Punta Arenas, Chile, the next day via Svalbard in Norway. Tracking these locations and keeping your shipboard firewall up to date becomes a major intensive task. Especially as the volume of content being transferred shore to ship is growing rapidly, as is the proportion of that content being hosted on a CDN. One also has to be very careful when using traditional firewall techniques that opening the firewall for one specific service does not mean opening the ship to third party content providers that share the same CDN.

The traditional firewall practice of identifying a service using IP addresses, ports and other network settings and maintaining these manually within the firewall portal simply does not work in these scenarios. The companies IT support staff will forever be chasing the termination point (or POP) of a specific service as their ships move around the Globe. So how does SnakeWall, SnakeWays' ground breaking shipboard firewall service, tackle this problem?

By using Artificial Intelligence. Hosted on the shipboard SnakeBox, independent of the existing shipboard IT networks, SnakeWall deploys machine learning techniques to identify, then actively monitor and control, access to any internet service. All that is needed from the IT support staff (or indeed the ship's crew) is to identify the domain name of that service and indicate whether they want it enabled or want it blocked. From that point on SnakeWall takes care of the rest, dynamically adjusting the firewall rules as and when required.

SnakeWall presents a very simple interface to the user and incorporates a pre-defined list of well-known maritime content providers such as the UK Hydrographic Office and the US Coast Guard. As the vessel moves around the globe SnakeWall tracks those services across their distribution networks learning about new local servers and automatically configuring firewall settings to allow access when and where required.

SnakeWall is one of the key modules in SnakeWays expanding portfolio of ship to shore connectivity services. It sits alongside SnakeMail, and naturally dovetails with our SnakeSwitch multi-network routing service. With the two combined, SnakeWall and SnakeSwitch, the ship is able to define separate firewall rules for multiple WAN circuits, VSAT, Inmarsat and Iridium for example, and for different shipboard LAN users, Ships' business, Crew and/or MTM. Once configured SnakeWall will control the firewall depending up the LAN/WAN combination currently in use. No need for any manual intervention when switching from Satellite to LTE for example.

Finally, SnakeDoor, our shore to ship remote access utility, allows you direct access to the SnakeBox and SnakeWall via one click in the SnakeCloud portal. Once connected via SnakeDoor you can (with the appropriate authority) modify any and all SnakeWall settings.

If you would like to know more about SnakeWays and our remote connectivity solutions please don't hesitate to contact me via LinkedIn or indeed directly at sales@SnakeWays.com. You can also visit our Website for more detailed information www.SnakeWays.com

Gregor G Ross

Chief Commercial Officer

SnakeWays GmbH