Opensystems

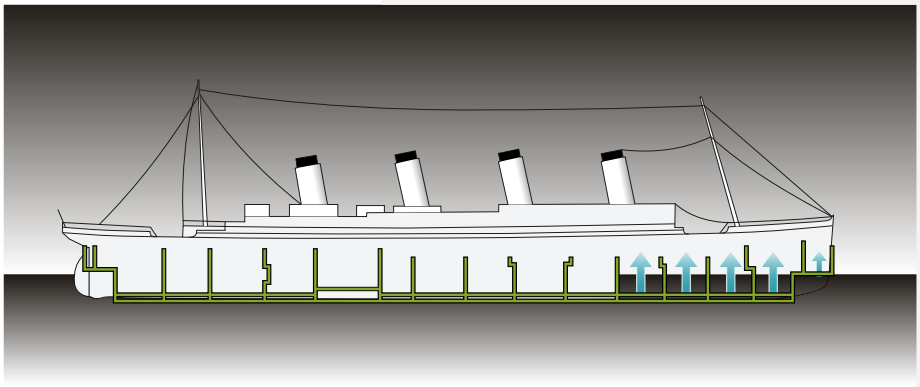
WHITE PAPER

SD-WAN – WHY WE SHOULD LEARN FROM THE TITANIC

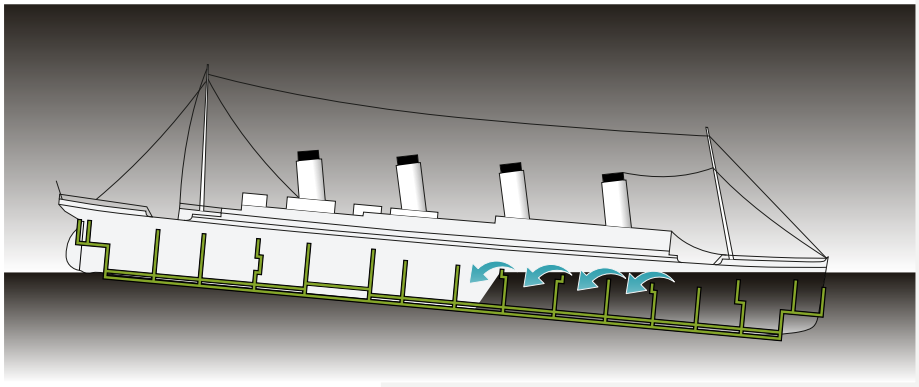
Navigating zoning concepts

What would have prevented the Titanic from sinking and how can we learn from it when designing a global WAN?

Author Martin Bosshardt



Damage caused by the collision with the iceberg affected five watertight compartments.



As each compartment filled, the bow sank deeper, and water flowed over the top of the bulkheads. With five compartments flooded, the ship could not survive.

A BIT OF HISTORY

At 882 feet (269 m) long, the Titanic was the second of the three Olympic-class ocean liners, which were by far the largest vessels of the British shipping company known as the White Star Line. In 1911, Shipbuilder magazine published an article about White Star Line's sister ships, Titanic and Olympic. The article described the construction of the ships and concluded that they were practically unsinkable.

On April 15, 1912, the Titanic sank after colliding with an iceberg during its maiden voyage.

The Titanic was separated into sixteen watertight compartments, with each compartment being watertight as long as the water did not reach a certain level. The compartments did not have a roof section, so they were more like individual containers without a lid. The ship was designed to survive flooding of four or fewer compartments simultaneously. When the iceberg sliced five compartments, those five sank deeper than the worst-case scenario the Titanic was designed for, and their neighboring compartments flooded as well.

NAVIGATING ZONING CONCEPTS

We find similar situations in many network designs today. Compartments, or in IT, the so-called zoning concepts are a security standard used in every datacenter design, and sometimes in LAN topologies, but almost never in a global WAN. In a centralized IT topology, security measures and control can be implemented and enforced centrally.

To utilize cloud and SaaS offerings, most companies are moving rapidly towards a decentralized application landscape. The data center is now out there in the cloud. In fact, it's no longer one data center, it's many data centers. And in most cases, we don't even know or have any control over where they are. Implementing agile SD-WAN topologies makes it possible to operate independently and use these services no matter when and where they are. That's the beauty of cloud services and the beauty of SD-WAN.

But that's where proven centralized security zoning concepts face their challenges. The WAN suddenly acts as a spillover between users, applications, or even legacy data centers. A simple attack can cause the outage of an entire enterprise organization. One of the prominent cases was certainly Maersk, which was shut down for 10 days by the outbreak of NotPetya.

EVERY USER AN OPENING TO THE SEA

SD-WAN design and security are no longer two separate disciplines. The design of the network defines, to a great extent, the security posture of any global organization. And the network itself becomes the most relevant security sensor in global distributed IT infrastructure.

Many organizations respond to these challenges with a vast number of new security products operated globally at all sites. In enterprise environments we find on average more than 35 different security products in operation. The goal of most of these products is to seal the boundaries. Companies hope to keep the enemy out or search for clues of compromise in correlating the logs from all those different tools. SIEM (security incident and event management) solutions try to bring light onto the white noise of all those logs. The result very often is the opposite. Too many products and too much complexity create challenging technology lifecycle management and hence more, rather than fewer, vulnerabilities. SIEM solutions produce too many false alerts by correlating logs from different products that are under constant update and change management, triggering false signals due to those changes.

It is usually a question of time and severity that forces us to deal with the fact that we are facing a compromised situation in some form. The attack vectors are thousandfold. Every user may be an opening to the sea. Most companies are dealing with a multitude of shadow IT applications that expose the entire enterprise to security standards it doesn't control. There are more than 25,000 applications out there that are easy to use for essentially every employee who has access to a browser – applications that may expose companies to software vendors and products you might have not even heard of.

RESILIENT STRUCTURE

To build a resilient SD-WAN, we must embrace the idea of being compromised. But we should also make sure that being compromised does not mean losing the entire ship. So, if designing an SD-WAN, try to think of the Titanic and try to think in terms of compartments, or zones.

Zoning becomes crucial to reducing complexity and zoning is key to building a resilient SD-WAN. Zoning allows you to keep attacks contained and buys you time to analyze and respond when a zone is compromised. An indicator of compromise will result in the isolation of a specific zone. This may limit certain functionalities but will not stall your entire operations. It allows you to respond while other zones are not affected. Zoning is the true beauty of SD-WAN and actually makes it possible for you to operate not just a single WAN but many WANs for every individual application or user group. There is no need for your finance department to work in the same zone as your production center or your warehouse. Or that your sales force works in the same network as your R&D department. Different zones require different security measures, and different zones require different triggers and measures to identify attacks.

So, if you design your SD-WAN, try to think of the Titanic. And try to think of zones without spillover. Those zones need to be isolated in case of compromise. You might want to let a compromised zone go, but you want to make sure you don't lose the entire ship.