CASE STUDY

Maritime Internet Services Provider Satisfies the Toughest Cybersecurity Demands

NexusOcean supplies broadband internet access to offshore energy and merchant shipping companies to meet their business needs and to support crew benefits programs. It also provides Voice over Internet Protocol (VoIP) and online entertainment. Satellite communications allow the crew—as well as a growing number of applications and hardware—to share data between offshore locations and the offices on shore.

Fast and Easy Access to Critical Business Applications

It is not just a matter of separating business traffic from the crew's personal communications. There is also the fact that high-priority business traffic always has to come first. "That is a challenge in management terms, because bandwidth onboard ships is simply limited," says Richard de Wit, founder and CEO of NexusOcean. "Depending on the service they opt for, we can provide our clients with unlimited internet via VSAT [very small aperture terminal], so there is no data limit. The client can also include a back-up or 4G connection, with unlimited data usage if desired, or just for specific protocols or applications. The costs per megabit can be significantly higher at sea than on land, so we went looking for a supplier who could help with this and ensure that our customers do not run any financial risks on that front. Our NexusOcean team attended various presentations by different suppliers, but Fortinet was the one that impressed them most."

"Fortinet allows you to manage the use of limited and expensive broadband to the maximum," de Wit continues. "Using Fortinet's Secure SD-WAN solution, we can establish the best possible channel for the traffic—over VSAT, 4G, or back-up connections—so we can have fast and easy access to critical business applications. Besides the SD-WAN functionality, this solution also comes with a wide range of security options to protect network traffic from cyber threats and prevent data loss or theft. We can offer our clients the best configuration to protect their IT environment; based on their specific needs we decide what is permitted and what is not."

In practice, NexusOcean configures the Fortinet devices at its own premises and then installs them onboard ship. "We want to avoid having to do that on site because ships only spend a limited time in any given port," de Wit explains. "So, we ensure the equipment is ready to go when they arrive on board. Installation is easy; even untrained

"The more you integrate Fortinet into your network and all your onboard hardware, the easier it all gets."

– *Richard de Wit, Founder and CEO, NexusOcean*

Details

Customer: NexusOcean

Industry: MSSP/Service Provider

Location: Vlissingen, The Netherlands

Business Impact

- Complies with IMO Guidelines for onboard cybersecurity
- Facilitates secure SD-WAN to manage and protect traffic via satellite
- Streamlines implementation and management of all Fortinet solutions for a single vessel or an entire fleet

personnel can handle it. Subsequent adjustments are made remotely using Fortinet's FortiManager [centralized management system]. We can modify, push, and control the configurations for a single ship or an entire fleet."

Risk Analysis Based on Onboard Network Use

The International Maritime Organization (IMO) created a security code in 1989, known as the ISM (International Safety Management) code. The IMO's stance is that more is needed than just measures governing physical safety; cybersecurity also needs to be addressed. This is especially important, given that the maritime industry happens to be a relatively easy target for cyber criminals. "That is because it is becoming more and more common for a ship's OT systems to be linked to an IT system these days," De Wit says. "This also makes the engine room and navigational equipment, for example, vulnerable to cyberattacks. The key issue is that the OT systems on ships often still run on outdated operating systems. You would be shocked at the number of things onboard that still work with Microsoft XP, an operating system no longer supported since November 2018."

The IMO is forcing shipping companies to focus on their network security. "That means they have to draft their own cyber response plans," De Wit comments. "They have to detail how network traffic is secured, with a firewall for instance, and which procedures and measures are in place to safeguard the systems and data. That requires making a risk assessment, and also being able to hand that over later on. Clear and comprehensible reporting about your cybersecurity capability is really essential to all of that. In 9 out of 10 cases, the standard reports produced by Fortinet's FortiAnalyzer solution already cover a major part of the IMO guidelines. The reports are generated automatically, and that is a big timesaver for our customers. The more you integrate Fortinet into your network and all your onboard hardware, the easier it gets."

De Wit believes Fortinet is one of the world's foremost experts in making risk analyses based on onboard network use. "FortiAnalyzer makes it possible for us to produce a report to back up our findings and to identify and pinpoint the weak spots. It also clarifies which measures need to be taken to close the gaps. Fortinet has fantastic tools to do all of that."

Solutions

- Fortinet Secure SD-WAN
- FortiManager
- FortiAnalyzer

"Using Fortinet's Secure SD-WAN solution, we can establish the best possible channel for the traffic—over VSAT, 4G, or back-up connections—so we can have fast and easy access to critical business applications."

– *Richard de Wit, Founder and CEO, NexusOcean*

September 4, 2020 7:51 AM

736636-0-0-EN

D:\Fortinet\Case Study\Red Case Study\Nexus Ocean\cs-FA-maritime-internet-services-provider-7242020