Global shipping giant enhances support for BYOD and cloud with Palo Alto Networks™

DIFFERENTIATION THROUGH SUPERIOR VALUE-ADDED SERVICE

Orient Overseas Container Line (OOCL) Limited is a wholly-owned subsidiary of Hong Kong Stock Exchange listed Orient Overseas (International) Ltd. Headquartered in Hong Kong, OOCL is one of the world's largest integrated international container transportation and logistics companies, linking over 60 countries including Asia, Europe, North America, the Mediterranean, the Indian sub-continent, the Middle East and Australia/New Zealand. OOCL is also an industry leader in the use of information technology and e-commerce to manage the entire cargo process.

PROVIDING SECURE NETWORK ACCESS FOR BYOD DEVICES USING THE CLOUD

With staff located in more than 270 offices around the world, ensuring reliable and secure access is a priority. Firewalls play an important role as the organization recognizes the vulnerabilities of sharing information across company networks. To protect the network, OOCL deployed a proxy server solution. However, the IT team quickly discovered that applications developed for the iPhone and iPad platforms were unsupported, including popular communication tools like Facetime. In some instances this had been limiting employee productivity levels.

In addition, with many employees based in remote locations around the world, the use of cloud-based services has also come to the fore in recent years. OOCL did not have enough visibility and access control over cloud applications used by its employees and was therefore unable to determine what content was passing through the network and what to prioritize given the limited and expensive international bandwidth.

With the company's existing firewall appliance approaching the end of its lifespan, this presented an opportunity for OOCL to reevaluate its strategy and consider alternative solutions. The IT department investigated available technologies in the market and after carefully evaluating several proposals chose the solution from Palo Alto Networks.

DEPLOYMENT CHALLENGES

Palo Alto Networks, working closely with its channel partners and the OOCL IT team, recommended replacing the proxy server and firewall solution with a fully redundant next-generation firewall solution that links all of the major offices and operations of the company worldwide.

OOCL

We take it personally

ORGANIZATION:
Orient Overseas Container Line Limited

INDUSTRY:
Shipping and Logistics

CHALLENGE:
Enhance visibility and control over BYOD users across more than 270 offices worldwide. Ensure that iPhone and iPad applications are able to work within the proxy server architecture. Gain visibility and access control over third-party cloud applications being used by employees. Replace aging firewall appliances that are nearing end of their lifespan.

SOLUTION:
The next-generation firewall solution comprises of two PA-5020, 48 x PA-500 and 20 x PA-200 firewalls deployed across more than 270 offices worldwide, delivering granular visibility of threats and better control of applications delivered via the cloud and across different devices.

RESULTS:
The increased application visibility and control, including cloud application, helps provide support for various client devices including personal devices like iPhones and iPads, which eased the security management of a complex information network covering over 270 offices worldwide.

paloalto NETWORKS

the network security company™

The Palo Alto Networks design encompassed three classes of firewall solutions deployed in pairs at major OOCL centers of operation worldwide. This included:

- Two PA-5020 firewalls: designed specifically for the data center, to be installed at the company's main data center in Hong Kong.
- Forty-eight PA-500 firewalls: optimized for large branch operations, were deployed at 24 of the company's largest operations worldwide.
- Twenty-two PA-200 firewalls: ideally suited for the much smaller office environment, for remote but critical business locations.

For a company with the size of OOCL, deployment of a new firewall solution of this scale presented some particular challenges. It needed to make sure that the integration of each pair of firewall solutions went smoothly with minimal or zero impact on operations, a vital aspect given as the company deals with time-sensitive production applications.

> *"Our success in global infrastructure depends on our ability to provide instant access to critical business information for employees regardless of where they are located and what device they are using to access the network. With the Palo Alto Networks solution, we are now able to provide a consistent, controlled and secure network connection for everyone."*
>
> **Steve Siu**
> **Director and CIO**
> **OOCL**

APPLICATION VISIBILITY AND CONTROL OVER ANY DEVICE AND PLATFORM

Traditional firewall solutions classify traffic by port and protocol. This was preventing OOCL from having visibility of application delivery. Visibility is important particularly when so many personal devices are being used to access company and customer data over the cloud.

However, each Palo Alto Networks next-generation firewall came with scalable route-based VPN and dynamic routing protocol support to enhance the resilience of OOCL's Virtual Private Network. Using the patent pending App-ID™ application classification technology from Palo Alto Networks, OOCL gained full visibility into, and policy control over, applications flowing in and out of its networks, regardless of port, protocol, SSL encryption, or evasive tactics. The User-ID™ technology available on Palo Alto Networks links IP addresses to specific user identities allowing OOCL to identify and control what applications are being used by each employee. The Content-ID technology identifies traditional and emerging threats – including those embedded in an SSL session – to facilitate total application access and usage control while enabling broad, real-time threat prevention.

In addition, the built-in Threat Prevention and Anti-virus features of the Palo Alto Networks firewall ensures that OOCL is able to achieve a consistent network security standard, rolling out policies and processes right across the entire organization, including at remote locations.

VISIBILITY ACROSS A NETWORK SPANNING 270 OFFICES IN 60 COUNTRIES

Fully deployed, the Palo Alto Networks solution gives OOCL greater visibility and control over what content it allows to traverse the company network, what applications are permitted to use the corporate network, and from which device. This will ensure that critical business applications will get bandwidth priority. IT will now be able to report on network activities down to the user level, and identify areas of improvement as well as anticipate future potential areas of investment.

With the next-generation firewall solution, protection and support for remote and mobile users is now provided with features for analyzing files for malware in a separate (cloud-based) portal that does not impact stream processing. Employees can leverage mobile applications and cloud services to increase productivity. At the same time, management will be able to more easily execute access control policies and processes and the higher visibility will enable it to better manage network utilization. With visibility and control, OOCL management can be assured that the company meets its compliance commitments.

As a global operation, remote locations use local ISPs when accessing company data. The experience is often not consistent and very dependent on the in-country service provider.

But with the Palo Alto Networks solution, different types of network traffic between offices can now ride on different ISPs' services depending on network quality and bandwidth requirements. OOCL will now be able to monitor ISP service capability and negotiate better terms and service at the country level. At the same time, a more consistent service experience can be achieved by tweaking network traffic down to the office level to compensate for any limitations in the ISP's service capability.

paloalto NETWORKS
the network security company™

3300 Olcott Street
Santa Clara, CA 95054

Main: +1.408.573.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com