



POWERING NEXT-GEN FIREWALLS WITH DPI AND ENCRYPTED TRAFFIC INTELLIGENCE

Elevating LANCOM's NGFW product capabilities with AI-powered DPI engine R&S®PACE 2 for advanced application filtering and policy enforcement

ROHDE & SCHWARZ

Make ideas real





CHALLENGE

Restoring traffic visibility lost to encryption

Encryption challenges and rising cybersecurity concerns demand real-time, dynamic application filtering and context-based security controls. LANCOM's suite of next-generation firewalls (NGFWs) harnesses the latest advancements in application and threat awareness from ipoque's next-gen deep packet inspection (DPI) engine R&S®PACE 2 to protect enterprise networks and ensure an undisturbed application experience.

The growing adoption of cloud, IoT and remote working, and the increasing prevalence of cyberattacks necessitate a comprehensive security framework to safeguard enterprise networks and resources. Given the growth in applications and attack vectors, a robust security framework must align its policies to the enterprise's risk profile and security posture. It also needs to ensure a highly optimized, context-based security implementation that balances threat management and network performance. This requires enterprises to put in place granular filtering policies that are based on application identity (e.g. critical enterprise applications) and corresponding behavioural thresholds (e.g. bandwidth consumed). It also requires these policies to be fine-tuned continuously based on the latest developments in application trends and the threat landscape.

LANCOM R&S®Unified Firewalls, a suite of next-gen UTM firewalls, provide a holistic security solution by combining multiple features such as IDS/IPS, SSL inspection and DPI. Using an intuitive web GUI, the firewalls enable enterprises to configure and calibrate their security policies with minimal errors, while keeping tabs on their network and secured devices.

In recent years, the emergence of tougher and stricter encryption and obfuscation protocols has progressively eroded the traffic visibility available to LANCOM Firewalls. Traditionally, the firewalls relied on the information embedded in SSL/TLS certificates to detect underlying traffic flows. With the advent of new encryption protocols such as TLS 1.3, this information is encrypted along with the packet payload. For instance, encryption of the Server Name Identifier data during a TLS handshake conceals the destination domain. Some encryption protocols such as ECH encrypt the entire handshake information. This impacts the effectiveness of traditional DPI tools, leaving major blindspots in its analysis. Without comprehensive analytics, LANCOM R&S®Unified Firewalls can no longer execute application-based policies in full, leading to inconsistencies in traffic filtering and additional layers of security processing. Inevitably, it also increases the network's susceptibility to threats, especially encrypted threats.

SUMMARY

Business area

- ▶ A leading European manufacturer of secure, reliable and future-proof networking and security solutions

Challenge

- ▶ Growing visibility gaps from newer and tougher encryption protocols such as TLS 1.3 impact the ability of NGFWs to execute intelligent traffic filtering and detect threats in real time, resulting in security vulnerabilities and policy inconsistencies.

Solution

- ▶ Embedding R&S®PACE 2, which comes with AI-based encrypted traffic intelligence (ETI), in LANCOM R&S®Unified Firewalls enables accurate application classification and advanced threat awareness, even across flows that are encrypted, obfuscated or anonymized.

Benefits

- ▶ By deploying R&S®PACE 2, LANCOM R&S®Unified Firewalls benefit from AI-enriched, next-gen DPI capabilities to tackle encrypted threats and enhance its overall ability to monitor, secure and optimize application traffic, including encrypted flows, while providing users an easy-to-access, intuitive interface.

SOLUTION

State-of-the-art protocol and application detection based on AI techniques

To address these challenges, LANCOM deployed ipoque's industry-leading DPI engine R&S®PACE 2 in its R&S®Unified Firewalls. R&S®PACE 2 merges advanced statistical and behavioral/heuristic analysis with encrypted traffic intelligence (ETI) to deliver traffic visibility up to application layer 7 and beyond, despite encryption, obfuscation and anonymization. ETI by ipoque leverages advanced machine learning and deep learning algorithms, such as k-NN, decision tree learning, CNN, RNN and LSTM. In doing so, it employs thousands of statistical, time series and packet-level features. In combination with high dimensional data analysis and advanced caching, ETI equips LANCOM R&S®Unified Firewalls with highly accurate and reliable classification of encrypted protocols, applications and services.

By leveraging R&S®PACE 2, LANCOM R&S®Unified Firewalls can implement intelligent and dynamic policies for application filtering, regardless of encryption, obfuscation and anonymization. This allows the firewalls to decide in real time which applications, application groups or protocols should be allowed, filtered or blocked in the network. Additionally, it enhances application-based routing, for example prioritization of critical enterprise applications, which helps to optimize network resources.

With a comprehensive, weekly updated library that boasts thousands of signatures, R&S®PACE 2 enables the firewalls to stay abreast of latest application trends. These updates incorporate new application releases, version upgrades and patterns of behavior across different devices and operating systems.

The benefits of licensing R&S®PACE 2

- ▶ Most efficient memory usage in the market
- ▶ Superfast filtering (avg. 14 Gbps throughput per core)
- ▶ ETI based on advanced ML/DL techniques
- ▶ Highest accuracy, even for encrypted traffic
- ▶ Always up-to-date, extensive signature library
- ▶ Ability to add custom signatures
- ▶ Seamless integration using a software-form factor
- ▶ First packet classification for instant identification
- ▶ Low TCO and high ROI
- ▶ 24/7 customer support

RESULT

Next-gen security and traffic control with application-based threat response

With R&S®PACE 2, LANCOM R&S®Unified Firewalls are able to distinguish all encrypted applications and services in real time and allocate appropriate policies accordingly, without depending on multiple filtering technologies. Not only does this restore full visibility into traffic flows, but it also cuts down monitoring overheads and complexities.

Similarly, by recognizing latest VPN, anonymization (e.g. CDN) and tunnelling protocols in the market, LANCOM R&S®Unified Firewalls are able to quickly identify traffic that is manipulated to conceal unauthorized activities. This is particularly important for enterprises handling a large remote workforce or huge volumes of IoT connections.

Apart from this, LANCOM can enhance application-based configurations, allowing customers to set fine-grained policy rules based on their risk appetite and the risk exposure of different enterprise and web applications. Customers can now define allowlists and blocklists and set different security responses to different security events. Leveraging the firewalls' superior interface, LANCOM can bring these capabilities seamlessly to customers' fingertips, which greatly improves their experience.

By licensing R&S®PACE 2, LANCOM not only saves significantly on development and maintenance costs, but also benefits from its continuous availability, joint strategic view and top-notch support.

"Network visibility is vital to ensure and optimize the functionality and operation of any network. Therefore, the use of application and network proxies has become much more important. The necessary data to resolve the aforementioned tasks can only be obtained by employing state-of-the-art encrypted traffic intelligence solutions."

Markus Irle, Vice President, Firewalls and Security at LANCOM

ipoque

ipoque, a Rohde&Schwarz company, is a global leader in the world of network analytics software. We leverage our deep domain expertise to create customized software solutions that empower our customers to transform data into intelligence. As a subsidiary of Rohde&Schwarz, we take advantage of potential synergies.

Rohde & Schwarz

The Rohde&Schwarz technology group is among the trailblazers when it comes to paving the way for a safer and connected world with its leading solutions in test&measurement, technology systems and networks&cybersecurity. Founded 90 years ago, the group is a reliable partner for industry and government customers around the globe. The independent company is headquartered in Munich, Germany and has an extensive sales and service network with locations in more than 70 countries.

Rohde & Schwarz GmbH & Co. KG

www.rohde-schwarz.com

ipoque GmbH

Augustusplatz 9 | 04109 Leipzig, Germany

Info: + 49 (0)341 59403 0

Email: info.ipoque@rohde-schwarz.com

www.ipoque.com

R&S® is a registered trademark of Rohde&Schwarz GmbH&Co. KG

Trade names are trademarks of the owners

PD 3673.0863.32 | Version 01.00 | August 2024

Powering next-gen firewalls with DPI and encrypted traffic intelligence

Data without tolerance limits is not binding | Subject to change

© 2024 Rohde&Schwarz GmbH&Co. KG | 81671 Munich, Germany

© 2024 ipoque GmbH | 04109 Leipzig, Germany