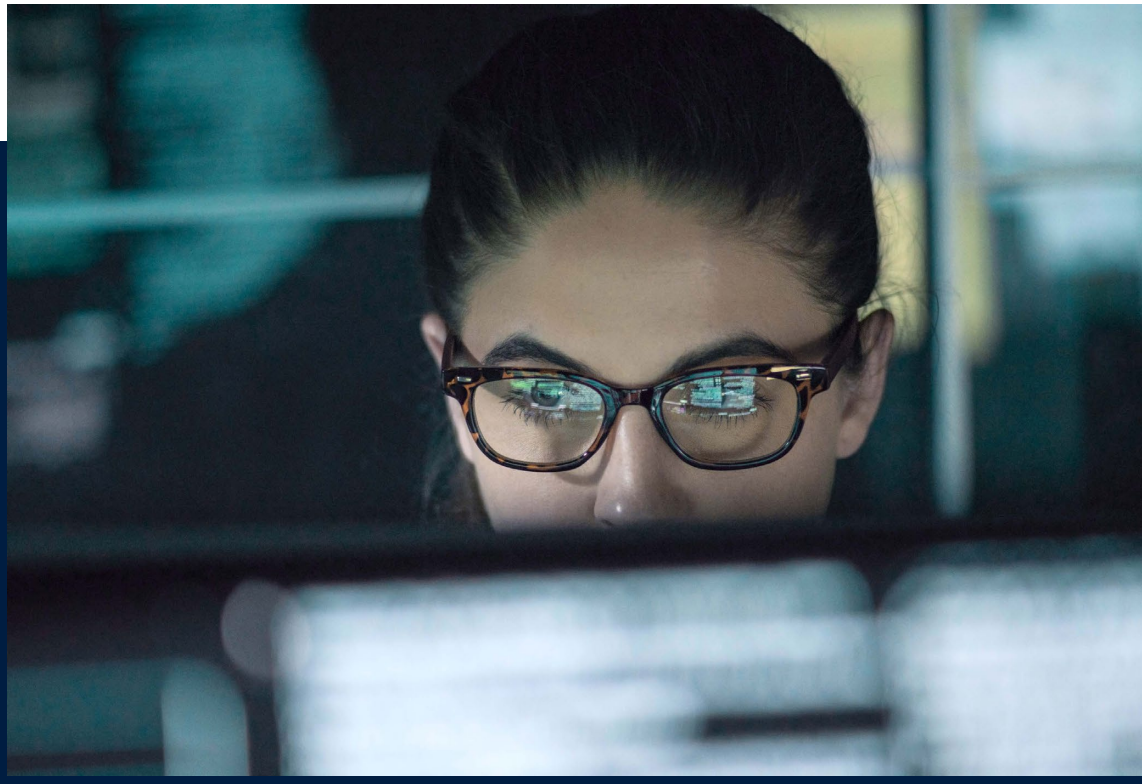
LANCOM SYSTEMS

Whitepaper

Next-Generation Deep Packet Inspection in LANCOM R&S®Unified Firewalls for reliable network transparency



Digital communications are increasingly complex: New technologies and ever stronger encryption technologies produce new risks and opportunities for IT managers. Efficiently managing the ever-growing amounts of network traffic and ensuring the best connectivity and highest security require granular network insights down to the application layer. But while individual applications used to be assigned to a dedicated port and could thus be easily managed via a port filter, this is no longer the case today. For this purpose, LANCOM R&S®Unified Firewalls use the R&S®PACE 2 Deep Packet Inspection (DPI) engine developed by R&S subsidiary ipoque. This detects applications quickly and reliably, so that they can be allowed, blocked or redirected as desired. This paper informs you about how this DPI engine assures the security of your network infrastructure.

What is Deep Packet Inspection?

Detailed filtering and validation of applications and protocols

Deep Packet Inspection (DPI) protects against cyber attacks and data leaks by precisely classifying the network traffic, protocols, and applications. In contrast to standard analysis technologies such as stateful packet inspection, which only checks the meta-data (header) of the data packets, DPI checks down to layer 7, i.e. the packet data itself. HTTPS data packets are also detected at a fine granular level by means of “Encrypted Traffic Analysis” This is the intelligent basis for easily setting up detailed security policies when operating certain applications via the LANCOM R&S®Unified Firewalls.

When do we use Deep Packet Inspection?

More transparency with increasing complexity

By precisely classifying network traffic at the application level (layer 7), a DPI engine gives IT managers full control over which applications are allowed or blocked in their network, for example with the Application Management integrated in UTM firewalls. To increase network performance, trusted applications can also be redirected straight to the Internet or to an external remote site by means of local breakouts.

What is R&S®PACE 2?

DPI engine for highest accuracy in IP traffic identification and classification

The industry-leading R&S®PACE 2 DPI engine is a software library that uses various technologies such as Deep Packet Inspection, pattern matching, behavioral and statistical analysis, and machine learning (ML) methods. The combination of these methods ensures the reliable and automatic identification and classification of thousands of network protocols and applications, including application characteristics and service types, in real time, including with encrypted or obfuscated IP traffic at application layer

7 and beyond. The R&S®PACE 2 DPI engine thus provides robust traffic analysis and comprehensive traffic management for cyber-threat protection by monitoring and controlling application performance.

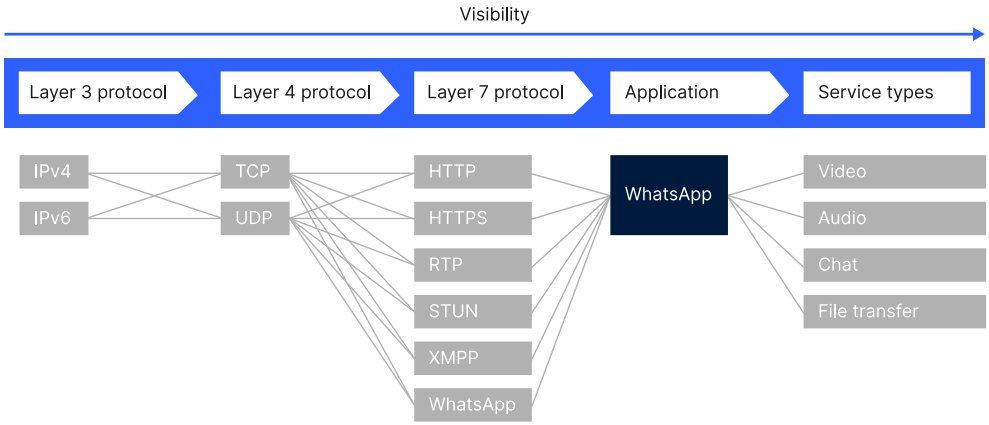


Figure 1:
Classifying IP traffic beyond layer 7

Developed by the R&S subsidiary ipoque for OEM use in security equipment, the future-proof DPI engine R&S®PACE 2 is licensed by LANCOM Systems for use in their LANCOM R&S®Unified Firewalls to provide state-of-the-art protocol and application detection. The licensing of this leading DPI technology guarantees field-tested top technology and thus the highest network security for companies and the public sector.

High accuracy of classification

The very broad classification portfolio is suitable for countless business and mobile applications and application services across all industries and regions. By using a variety of cutting-edge classification techniques, R&S®PACE 2 offers the highest detection rate of network protocols and applications on the market, even with advanced obfuscation and encryption and beyond layer 7. Thanks to the feedback and demands from customers all over the world, R&S®PACE 2 provides a very low false negative rate, i.e. unrecognized applications. What this means is: Very high traffic-detection accuracy and reliability with virtually no false positives. The constant observation for new versions of applications and their behavior on different devices, with different operating systems and in different networks ensures high accuracy in the classification of applications at all times.

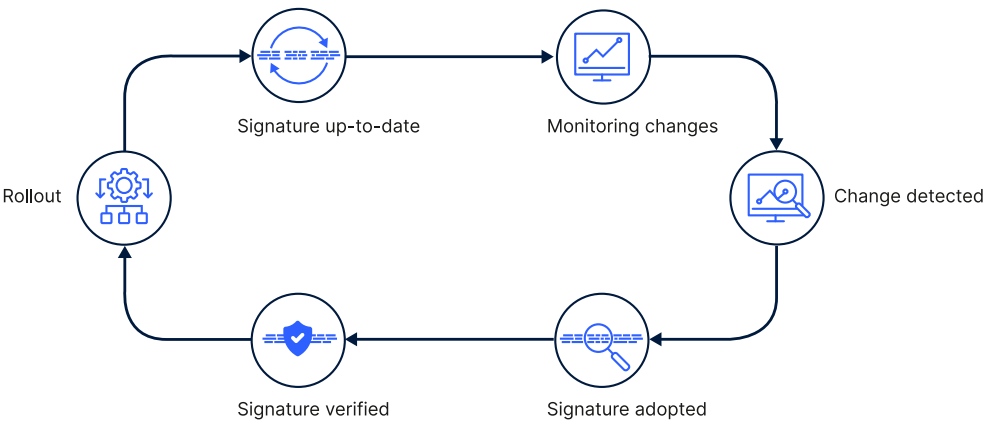


Figure 2:
R&S®PACE 2 update process when applications and protocols change

Using the R&S®PACE 2 in Next-Generation Firewalls (NGFW)

Encryption and obfuscation, the Internet of Things, the cloud, and the increasing number of mobile employees with their own devices in the company network (Bring Your Own Device, BYOD) are just a few of the challenges that a modern firewall has to meet. Next-generation firewalls therefore provide granular insights into IP traffic to identify threats and protect users from rapidly evolving new cyber threats.

R&S®PACE 2 enables LANCOM R&S®Unified Firewalls to easily distinguish between secure and malicious traffic while offering the highest accuracy of protocol and application classification on the market—including business, messaging, and IoT applications. Furthermore, in market comparisons the R&S®PACE 2 detects the most VPN, anonymization, and tunneling protocols.

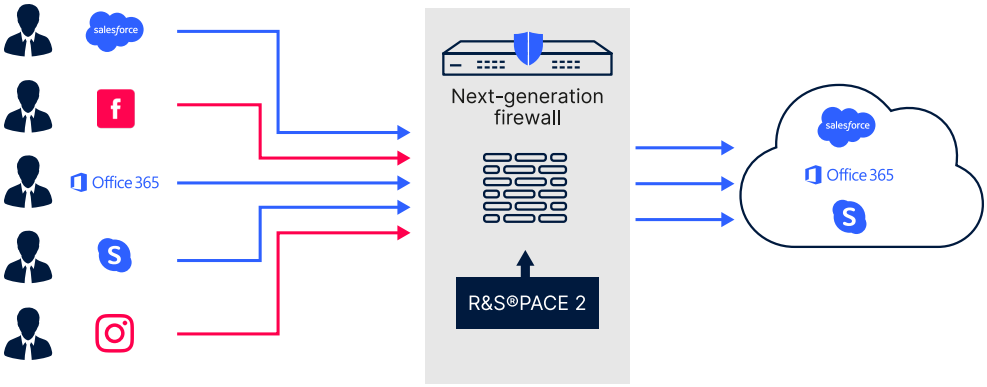


Figure 3:
Application control via R&S®PACE 2 in NGFWs

Conclusion

The R&S®PACE 2 DPI engine offers the top technology required to ensure reliable network security in an increasingly complex threat environment. Even new applications are recognized and classified into safe and malicious data traffic.

More about the LANCOM R&S®Unified Firewalls and their security features and management tools can be found at www.lancom-systems.com/products/security.

LANCOM Systems GmbH
A Rohde & Schwarz Company
Adenauerstr. 20/B2
52146 Wuerselen | Germany
info@lancom.de | lancom-systems.com