



LANCOM
SYSTEMS

Whitepaper

Next-Generation Deep
Packet Inspection in
LANCOM R&S®Unified
Firewalls für zuverlässige
Netzwerktransparenz





Digitale Kommunikation wird zunehmend komplex: Neue Technologien und immer stärkere Verschlüsselungstechnologien führen zu neuen Risiken und Chancen für IT-Verantwortliche. Um den ständig wachsenden Netzwerkverkehr effizient zu verwalten und die beste Konnektivität und höchste Sicherheit zu gewährleisten, sind granulare Netzwerkeinblicke bis auf die Anwendungsebene erforderlich. Doch während früher einzelne Anwendungen einem dedizierten Port zugeordnet und somit einfach über einen Portfilter verwaltbar waren, ist dies heute nicht mehr der Fall. Zu diesem Zweck kommt in LANCOM R&S®Unified Firewalls die von der R&S-Tochter ipoque entwickelte Deep Packet Inspection (DPI)-Engine R&S®PACE 2 zum Einsatz, um Anwendungen schnell und zuverlässig erkennbar zu machen und wie gewünscht zu erlauben, zu blockieren oder umzuleiten. Wie diese DPI-Engine die Sicherheit Ihrer Netzwerkinfrastruktur garantiert, erfahren Sie in diesem Paper.

Was ist Deep Packet Inspection?

Detaillierte Filterung und Kontrolle von Anwendungen und Protokollen

Deep Packet Inspection (DPI) ermöglicht den Schutz vor Cyberangriffen und Datenlecks durch eine präzise Klassifizierung des Netzwerkverkehrs sowie der eingesetzten Protokolle und Anwendungen. Im Gegensatz zu herkömmlichen Analysetechnologien wie Stateful Packet Inspection, die nur die Metadaten (Header) der Datenpakete analysiert, überprüft DPI die bis auf Layer 7-Ebene, also den Datenbereich des Datenpakets. Durch eine „Encrypted Traffic Analysis“ werden auch HTTPS-Datenpakete feingranular erkannt. Dies ist die intelligente Basis für die einfache Einrichtung auch detaillierter Sicherheitsrichtlinien zur Verwendung bestimmter Anwendungen über die LANCOM R&S®Unified Firewalls.

Wann kommt Deep Packet Inspection zum Einsatz?

Mehr Transparenz bei steigender Komplexität

Durch die präzise Klassifizierung des Netzwerkverkehrs auf Anwendungsebene (Layer 7), ermöglicht eine DPI-Engine IT-Verantwortlichen beispielsweise über ein auf UTM-Firewalls integriertes Application Management selbst zu entscheiden, welche Anwendungen in ihrem Netzwerk erlaubt oder blockiert werden sollen. Zur Steigerung der Netzwerk-Performance können vertrauenswürdige Anwendungen ebenfalls durch sogenannte Local Breakouts direkt ins Internet oder zu einer externen Gegenstelle umgeleitet werden.

Was ist R&S®PACE 2?

DPI-Engine für höchste Identifizierungs- und Klassifizierungsgenauigkeit des IP-Verkehrs

Die branchenführende R&S®PACE 2 DPI-Engine ist eine Softwarebibliothek, die verschiedene Technologien wie Deep Packet Inspection, Pattern-Matching, Verhaltens- und statistische Analyse sowie Methoden des maschinellen Lernens (ML) einsetzt. Durch die Kombination dieser Verfahren werden tausende von Netzwerkprotokollen und Anwendungen, einschließlich Anwendungsmerkmalen und Diensttypen, zuverlässig und automatisiert in Echtzeit identifiziert und klassifiziert, selbst bei verschlüsseltem oder verschleiertem IP-Datenverkehr auf Anwendungsebene Layer 7 und darüber hinaus. So bietet die R&S®PACE 2 DPI-Engine durch Überwachung und Steuerung der Anwendungsleistung eine zuverlässige Verkehrsanalyse und ein umfassendes Verkehrsmanagement für den Schutz vor Cyberbedrohungen.

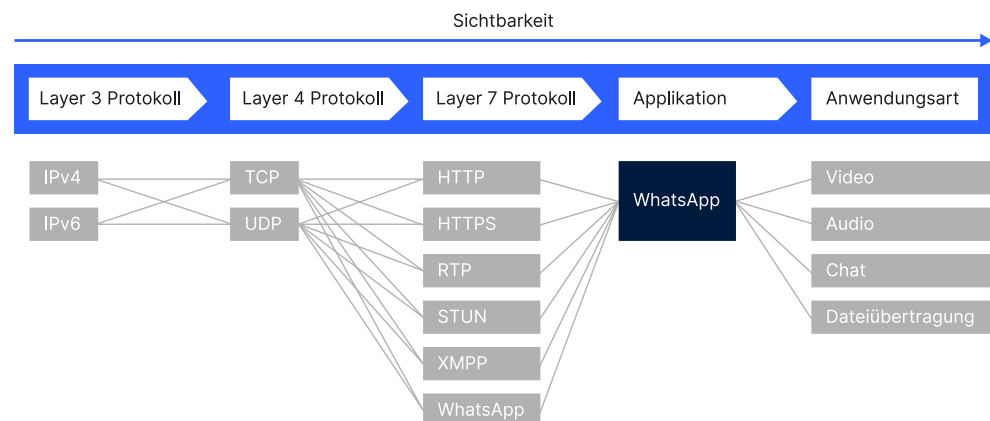


Abbildung 1:
Klassifizierung des
IP-Datenverkehrs über
Layer 7 hinaus

Entwickelt von der R&S-Tochter ipoque für den OEM-Einsatz in Sicherheitsequipment, wird die zukunftssichere DPI-Engine R&S®PACE 2 von LANCOM Systems für den Einsatz in den LANCOM R&S®Unified Firewalls lizenziert, um diese mit modernster Protokoll- und Anwendungserkennung auszustatten. Die Lizenzierung dieser führenden DPI-Technologie garantiert felderprobte Top-Technologie und somit höchste Sicherheit der Netzwerkinfrastruktur für Unternehmen und den öffentlichen Sektor.

Hohe Klassifizierungsgenauigkeit

Das sehr breite Klassifizierungsportfolio eignet sich für unzählige Geschäfts- und mobile Anwendungen und Anwendungsdienste über alle Branchen und Regionen hinweg. Durch den Einsatz einer Vielzahl modernster Klassifizierungstechniken bietet R&S®PACE 2 die am Markt höchste Erkennungsrate von Netzwerkprotokollen und Anwendungen, selbst bei fortgeschrittener Verschleierung und Verschlüsselung und über Layer 7 hinaus. Dank des Feedbacks und der Anforderungen von Kunden auf der ganzen Welt hat R&S®PACE 2 eine sehr niedrige False-Negative-Rate, d. h. eine sehr niedrige Rate an nicht erkannten Anwendungen. Das bedeutet: Sehr hohe Erkennungsgenauigkeit und -zuverlässigkeit

des Datenverkehrs mit praktisch keinen False Positives. Die ständige Beobachtung neuer Versionen von Anwendungen und deren Verhalten auf unterschiedlichen Geräten, mit unterschiedlichen Betriebssystemen und in unterschiedlichen Netzen gewährleistet jederzeit eine hohe Genauigkeit bei der Klassifizierung von Anwendungen.

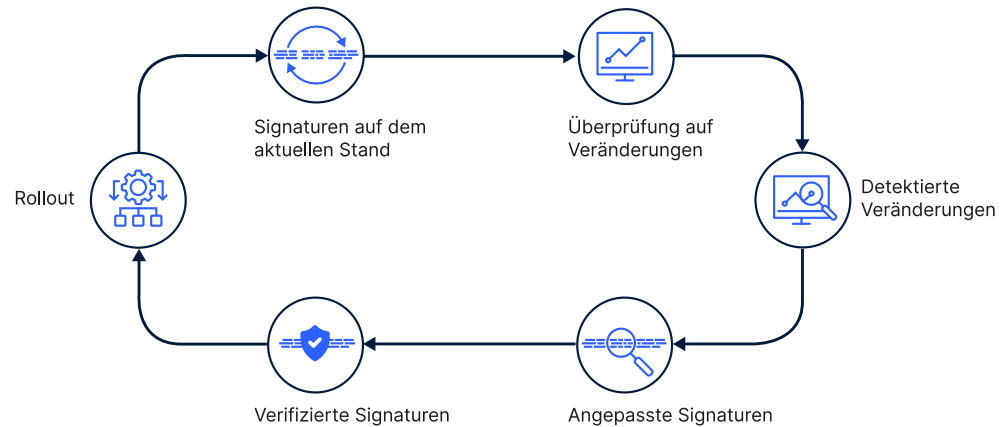


Abbildung 2:
Aktualisierungsprozess
der R&S®PACE 2
bei Änderungen
von Anwendungen
und Protokollen

Anwendung der R&S®PACE 2 in Next-Generation Firewalls (NGFW)

Verschlüsselung und Verschleierung, das Internet der Dinge, die Cloud sowie die zunehmende Zahl mobiler Mitarbeitenden mit eigenen Geräten im Unternehmensnetzwerk (Bring Your Own Device, BYOD) sind nur einige der Herausforderungen, denen eine moderne Firewall begegnen muss. Next-Generation Firewalls gewähren daher granulare Einblicke in den IP-Datenverkehr, um Bedrohungen gezielt zu identifizieren und Anwender vor den sich schnell entwickelnden neuen Cyberbedrohungen zu schützen.

Mit R&S®PACE 2 können LANCOM R&S®Unified Firewalls leicht zwischen sicherem und böartigem Datenverkehr unterscheiden und dabei die höchste Protokoll- und Anwendungsklassifizierungsgenauigkeit auf dem Markt nutzen – einschließlich Geschäfts-, Messaging- und IoT-Anwendungen. Darüber erkennt R&S®PACE 2 im Marktvergleich die meisten VPN-, Anonymisierungs- und Tunneling-Protokolle.

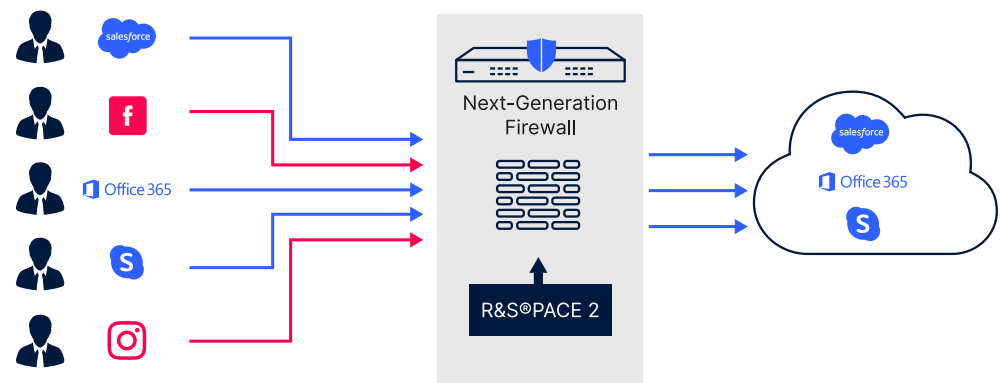


Abbildung 3:
Anwendungskontrolle über
R&S®PACE 2 in NGFWs



Fazit

Um eine zuverlässige Netzwerksicherheit in einer zunehmend komplexeren Bedrohungslage zu gewährleisten, bietet die R&S®PACE 2 DPI-Engine die notwendige Top-Technologie. Dabei werden auch neuartige Anwendungen erkannt und in sicheren und böartigen Datenverkehr klassifiziert.

Mehr zu den LANCOM R&S®Unified Firewalls und Ihren Sicherheitsfeatures und Management-Tools finden Sie unter www.lancom-systems.de/produkte/security.