LCOS FX 10.5

Passgenaue Sicherheit für die Netzwerke kleiner Büros, Schulen und größerer Unternehmen

LCOS FX 10.5 bietet für die LANCOM R&S®Unified Firewalls ein starkes Paket sowohl für kleinere Firmen, für Bildungseinrichtungen als für auch größere Unternehmen: E-Mail-Schutz bei Einsatz extern gehosteter IMAP-Server, die zeitliche Aufhebung von Content-Filter-Regeln für den Schulunterricht und ein feingranulares anwendungsbasiertes Routing sind die Highlights der neuen Firmware. Damit unterstreichen die LANCOM R&S®Unified Firewalls einmal mehr ihren Ruf als optimale Komplettlösung für state-of-the-art Sicherheit und Unified Threat Management (UTM) kleiner und mittelständischer Unternehmen.

- IMAP-Proxy – für umfassende E-Mail-Sicherheit
- Content-Filter Override – Erlaubnis vorübergehend erteilen
- Application Based Routing – Bandbreiten und Routen gezielt verteilen
- Desktop-Suche – Der Desktop-Tags-Filter wird zum Desktop-Filter erweitert
- Regeln aus dem Protokoll erstellen – Aus Alarm- oder System-Protokolleinträgen direkt neue Regeln erstellen
- Wiederherstellungspunkte – Einfaches Rücksetzen der Firewall auf die vorherige Version
- VPN-SSL-Bridging – Netze an unterschiedlichen Standorten sicher und zuverlässig auf Layer-2 miteinander verbinden
- Mehrere angemeldete Administratoren

LANCOM Systems

LCOS FX LANCOM Operating System

LCOS FX 10.5 Highlights	
IMAP-Proxy	Gerade für Anwender, die keinen eigenen E-Mail-Server betreiben, sondern Ihren E-Mail-Verkehr über einen externen Dienstleister abwickeln, ist das IMAP-Protokoll sehr interessant. E-Mails werden auf dem Server des Anbieters bearbeitet, wodurch die jeweilige Nachricht auf allen Endgeräten in gleicher Version vorliegt. Nun steht den LANCOM R&S®Unified Firewalls erstmals auch ein IMAP-Proxy zur Verfügung mit dem das komplette Nachrichtenaufkommen des IMAP-Servers auf Trojaner, Viren und andere Bedrohungen untersucht wird. Spam-Mails werden erkannt und aussortiert. Selbst Zero-day-Schutz ist dank der Nutzung von Sandboxing und Machine Learning der Firewalls möglich.
Content-Filter Override	Gerade in Schulnetzwerken ist ein Content-Filter unerlässlich. Schüler sollen vor jugendgefährdenden oder gesetzeswidrigen Inhalten geschützt werden und auch der Besuch von ansonsten unproblematischen Webseiten und Inhalten kann schnell zur großen Ablenkung im Unterricht beitragen. Doch wenngleich es sinnvoll ist, beispielsweise YouTube während der Unterrichtszeiten zu blockieren, kann die Nutzung dieses Dienstes punktuell auch während der Schulstunde Sinn ergeben. Hierzu kann nun die Lehrperson einen Code an ihre Schüler versenden, mit dem die festgelegte Filterregel zeitweise außer Kraft gesetzt wird. Sobald die Unterrichtsstunde beendet ist, greift die Filterregel erneut und verwehrt den Zugang zur Website oder Anwendung.
Application-based Routing	Mittels PACE2 DPI Engine können erkannte Protokolle und Applikationen gezielt geroutet werden. Hierfür stehen drei verschiedene Möglichkeiten zur Verfügung. So kann in einem bestimmten Multi-WAN-Szenario für bestimmte ausgehende Verbindung gezielt die nutzbare Leitung ausgewählt werden und beispielsweise Streaming-Dienste über die langsamere Leitung, VPN jedoch als Träger geschäftskritischer Datenverkehre zwischen Filiale und Zentrale über die schnellere Leitung geroutet werden. Vertrauenswürdige Cloud-Applikation können vom Proxy ausgenommen oder bestimmte Applikationen statt über IPSec-Tunnel direkt am Filialstandort zum Anbieter ausgeleitet werden, obwohl der restliche Internetverkehr über eine sichere Verbindung zur Zentrale geschickt wird.
Weitere Features	
Desktop-Suche	Der Desktop-Tags-Filter wird zum Desktop-Filter erweitert. Hierüber kann nun sowohl nach Desktop-Objekten als auch nach Desktop-Verbindungen gesucht werden. Nicht zutreffende Objekte und Verbindungen werden dabei ausgeblendet. Über diese Funktion kann nach einer Vielzahl von Parametern gesucht werden wie beispielsweise Name des betreffenden Desktop-Objektes, IP-Adressen, Netzwerke und Bereiche, VPN-SSL-Verbindungsnamen oder Proxy-Flags.
Regeln aus dem Protokoll erstellen	Aus Alarm- oder System-Protokolleinträgen über abgewiesene Zugriffe können direkt neue Regeln erstellt werden. Wenn die Firewall mit den aktuellen Regeln beispielsweise bestimmten Netzwerkverkehr blockiert, der eigentlich erwünscht ist, kann anhand des entsprechenden Protokolleintages mit wenigen Klicks eine neue Regel erstellt werden, die den Verkehr zukünftig erlaubt.
Wiederherstellungspunkte	Das Upgrade auf die nächste Firmware-Version ist nun kein Grund mehr zur Besorgnis. Bevor der Vorgang startet, wird automatisch ein Wiederherstellungspunkt erzeugt. Sollte danach nicht alles zur vollsten Zufriedenheit funktionieren, setzen Sie Ihre Firewall einfach auf den funktionierenden Ausgangszustand zurück.
VPN-SSL-Bridging	Mittels dieser Funktion können nun zwei oder auch mehrere Netze an unterschiedlichen Standorten ganz sicher und zuverlässig auf Layer-2 miteinander verbunden werden. Die beiden voneinander entfernten Netze agieren dadurch untereinander wie ein Netz und eine Kommunikation nicht IP-basierter Protokolle kann dazwischen stattfinden.
Mehrere angemeldete Administratoren	Jetzt ist es möglich, dass mehrere Administratoren zur gleichen Zeit im Webclient der LANCOM R&S®Unified Firewall angemeldet sind. Dabei erhält lediglich der zuerst angemeldete Administrator auch Schreibrechte und kann somit Änderungen an der Konfiguration vornehmen. Alle weiteren Administratoren erhalten ausschließlich Leserechte. Sobald sich der erste abmeldet, wird das Schreibrecht an den nächstangemeldeten Administrator übertragen. Eine deutliche Vereinfachung gerade in größeren Administrationsteams.
LCOS FX 10.4 Highlights	
Setup Wizard	Mit dieser Release-Version erhält die Firewall einen intuitiv zu bedienenden Installationsassistenten, der eine einfache Erstkonfiguration mit nur wenigen Mausklicks in weniger als fünf Minuten erlaubt. Richten Sie den Internetzugang, die IP-Adress-Zuweisung sowie UTM-Funktionen wie Anti-Malware, IDS/IPS, URL- und Content-Filter einfach ein.
Cloud-managed Firewall	Die LANCOM R&S®Unified Firewalls sind nun Cloud-ready! Ein einfacher und zugleich sicherer Pairing-Prozess via PIN oder Aktivierungscode verbindet die Geräte mit der LANCOM Management Cloud (LMC). Sie werden daraufhin in der Geräteübersicht angezeigt, was ein übersichtliches Monitoring und eine Alarmierungsfunktion über den Gerätezustand erlaubt. Per Web-Tunnel kann aus der LMC auf die Managementoberfläche der Firewalls zugegriffen und eine Fernkonfiguration vorgenommen werden.
Weitere Features	
Layer-7-Anwendungsverwaltung in der LANCOM Management Cloud	Über die LMC können mit den Firewalls nun stand-alone oder in Verbindung mit LANCOM Routern Regeln erstellt und anschließend auf die einzelnen Standorte ausgerollt werden, mithilfe derer einzelne Applikationen geblockt oder ein direkter Zugriff erlaubt werden kann.
Ready-to-use-Integration des LANCOM Advanced VPN Client	Mit diesem Firmware-Release ist jetzt eine einfache Erstellung von schlüsselfertigen Importprofilen für den LANCOM Advanced VPN Client möglich. Diese Profile werden als *.ini-Datei ausgegeben können mit wenigen Schritten in den Client importiert werden. Dieser baut anschließend eine sichere VPN-Verbindung über das verfügbare Verbindungsmedium zur Gegenstelle auf.
Alarmierung und E-Mail-Benachrichtigung	Die Firewalls versenden ab dieser Firmware-Version E-Mails mit Informationen über wichtige Ereignisse. Das kann wahlweise sofort bei Eintritt des Ereignisses oder aggregiert erfolgen. Dabei ist für jeden Ereignis-Typ konfigurierbar, wie häufig ein E-Mail-Versand erfolgen soll. Versand-Ereignisse sind z.B. Unterbrechung und Wiederaufbau von Netzwerkverbindungen, Firewall-Neustarts oder High Availibility Switch-over.
Benutzerspezifische Applikationsfilter-Regeln	Die LANCOM R&S®Unified Firewalls unterstützen ab diesem Firmware-Release auch die Kombination aus Benutzerauthentifizierung und Applikationsfilter. Das bedeutet, dass bestimmten Gruppen oder gar einzelnen Personen im Unternehmen bestimmte Applikationsregeln zugeordnet werden können.

LANCOM Systems

LCOS FX LANCOM Operating System

Allgemeine Features	Basic License	Full License	Feature-Beschreibung
Contentfilter	nur UF-50	✓	> Filtern nach URL und Inhalt > Anpassbare Regeln für Benutzer > Blacklists / Whitelists > Import / Export von URL-Listen > Kategoriebasiertes blockieren von Websites (individuell konfigurierbar) > Online-Scan-Technologie > HTTP(S)-Proxy-Unterstützung > Override-Funktion (wahlweise allgemein oder per zeitlich begrenztem Override-Code)
Applikationskontrolle*		✓	> Layer-7-Paketfilter (DPI – Deep Packet Inspection) > Filtern nach Applikationen (z. B. Facebook, YouTube, BitTorrent etc.) > Blacklists / Whitelists > Protokollvalidierung > Routing per Applikation > HTTP und IEC 104 Dekodierer > R&S®PACE 2 (Protocol and Application Classification Engine) > *) verfügbar für LANCOM R&S®Unified Firewall UF-200, UF-300, UF-500 und UF-900
Antivirus*		✓	> HTTP/S, FTP, IMAP/S, POP3/S, SMTP/S > Ausnahmen konfigurierbar > Mehrstufiges Scan-Konzept (lokal, sowie Cloud-basiert) > Sandboxing > Schnelle Klassifizierung von Zero-Day-Bedrohungen durch AI-Technologien (Machine Learning) > *) verfügbar für LANCOM R&S®Unified Firewall UF-100, UF-200, UF-300, UF-500 und UF-900
Antispam*		✓	> IMAP/S, POP3/S, SMTP/S > Definierbare Scanstufen > GlobalView Cloud unter Verwendung von Recurrent Pattern Detection (RPD) – Spamerkennung auf Basis des Verteilungsmusters der E-Mails > Blacklists / Whitelists > Automatische Zurückweisung / Löschung von E-Mails > *) verfügbar für LANCOM R&S®Unified Firewall UF-100, UF-200, UF-300, UF-500 und UF-900
IDS (Intrusion Detection System) / IPS (Intrusion Prevention System)*		✓	> Schutz vor DoS (Denial of Service), Portscan, Malware, Botnets, Exploits und Schwachstellen > Mehr als 40.000 aktive Signaturen > konfigurierbare Ausnahmen > Scanning aller Schnittstellen > *) verfügbar für LANCOM R&S®Unified Firewall UF-200, UF-300, UF-500 und UF-900
Proxies	HTTP VoIP	✓	> HTTPS, FTP, IMAP/S, POP3/S, SMTP/S, SIP > HTTP (transparent / nicht transparent) > Reverse Proxy > Unterstützt Active Directory und lokale Benutzer > Zeitgesteuert
VLAN	✓	✓	> 4096 VLANs pro Schnittstelle > 802.1q Header-Tagging (paketbasierte tagged VLANs) > Kompatibel mit Bridging
Bridge-Modus	✓	✓	> Layer-2-Firewall-Funktion > Spanning Tree (Bridge ID, Port-Kosten) > Unbegrenzte Anzahl von Schnittstellen pro Bridge
Monitoring & Statistiken	✓	✓	> Statistiken (IDS / IPS, Applikationskontrolle, Surfkontrolle, Antivirus / Antispam) > Protokollierung zu externen Syslog-Servern > Exportieren als CSV- und XLS-Dateien > SNMP/v2c und v3 > Connection Tracking
Administration	✓	✓	> Objektorientierte Konfiguration > Rollenbasierte Administration > CLI (Command-line interface) über SSH > Desktop als PDF und HTML speichern > IP-Basierte Zugriffbeschraenkung fuer SSH und Webclient > Simultaner Zugriff mehrerer Administatoren (einer lesend und schreibend, weitere nur lesend)
Web-Interface	✓	✓	> Selbsterklärende Funktionen > Praktischer Wizard zur Ersteinrichtung > Überblick über das gesamte Netzwerk > Übersicht über alle aktiven Dienste > Browserbasiert und plattformunabhängig > Optimales Filtern der Ansicht auf Grundlage benutzerdefinierter Tags
QoS	✓	✓	> Garantierte QoS-Bandbreite konfigurierbar für Internetverbindungen > QoS mit ToS-Flags > QoS in VPN-Verbindungen

LCOS FX LANCOM Operating System

Allgemeine Features (Fortsetzung)	Basic License	Full License	Feature-Beschreibung
X.509-Zertifikate	✓	✓	> CRL (Certificate Revocation List) – Zertiffikatsperrliste für ungültige Zertifikate > OCSP (Online Certificate Status Protocol) – Netzwerkprotokoll zur Statusvalidierung von X.509-Zertifikaten > Multi-CA-Unterstützung > Unterstützung von Multi-Host-Zertifikaten
VPN	✓	✓	> Benutzerauthentifizierung > Hochverfügbarkeit > Site-to-Site und Client-to-Site > Client-Konfigurationspakete
IPSec	✓	✓	> Volltunnel-Modus > IKEv1, IKEv2 > PSK (Pre-Shared Key) / Zertifikate > DPD (Dead Peer Detection) > NAT-T > XAUTH, L2TP > Portkonfiguration
SSL-VPN	✓	✓	> Routing-Modus VPN > Bridge-Modus VPN > TCP / UDP > Spezifikation von WINS- und DNS-Servern
Backup und Wiederherstellung	✓	✓	> Lokaler oder Fernzugriff > Automatischer Import während der Installation > Automatische und zeitbasierte Backups > Automatischer Upload (FTP, SCP) > Automatischer Fallback bei Upgrade-Problemen > Desaster-Recovery via USB-Stick
Benutzerauthentifizierung	✓	✓	> Active Directory-Import > Lokale Benutzerverwaltung > Authentifizierung über Web oder Client > Single Sign-On (Kerberos) > Mehrere Anmeldungen > Captive-Portal > Terminal Server Support (über Remote Desktop IP Virtualisierung)