LCOS FX 10.13

Addendum

09/2023

LANCOM SYSTEMS

Inhalt

Copyright

LANCOM Systems GmbH

Adenauerstr. 20/B2

52146 Würselen

Deutschland

www.lancom-systems.de

1 Addendum zur LCOS FX-Version 10.13

Dieses Dokument beschreibt die Änderungen und Ergänzungen in der LCOS FX-Version 10.13 gegenüber der vorherigen Version.

2 Regelvererbung

Der Dialog für eine Verbindung zwischen zwei Desktop-Objekten wurde überarbeitet und mit neuen Funktionen erweitert. Im oberen Bereich werden zusätzliche Informationen für die verbundenen Desktop-Objekte angezeigt. z. B. verwendetes Interface oder IP-Adresse.

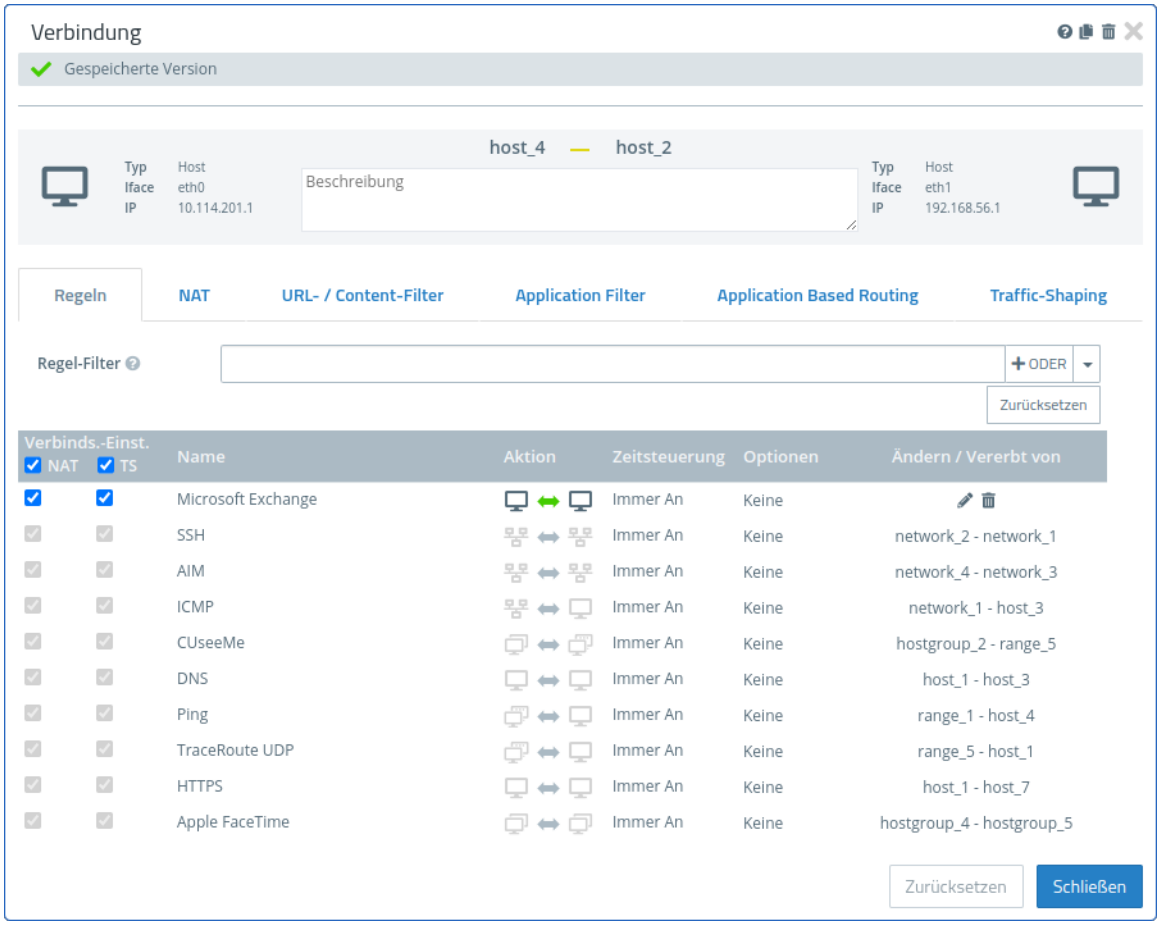

Abbildung 1: Verbindung zwischen Desktopobjekten

Wie bisher werden die ausgewählten Dienste in der Tabelle im Tab **Regeln** angezeigt. Außerdem werden nun auch die Regeln angezeigt, die zwischen übergeordneten Objekten konfiguriert sind. Diese vererbten Regeln können nicht direkt editiert werden. Mit Klick auf den Namen der Regel können aber die Einstellungen für diese Regeln angesehen werden. In der Spalte **Ändern / Vererbt von** werden statt den Editier-Buttons die Namen der Verbindungen angezeigt, aus denen diese Regeln verwendet werden. Mit Klick auf diese Namen, kann die dazugehörige Verbindung direkt geöffnet werden.

Über die Filterfunktion können Sie die Anzeige der Regeln einschränken, so dass Sie schneller feststellen können, ob eine bestimmte Regel bereits vorhanden ist. Filterkriterien sind

- Text für Namen, Regelnamen, Verbindungsnamen und Protokolle
- Zahlen für Ports und Portbereiche
- Booleans z. B. für DMZ, Proxy oder NAT

3 LANCOM Trusted Access

Im Rahmen von LANCOM Trusted Access (LTA) gibt es einige Ergänzungen, um die Einstellungen, die von der LANCOM Management Cloud kommen, sinnvoll darstellen zu können. Für LANCOM Trusted Access werden die Zugriffregeln in der LANCOM Management Cloud konfiguriert. Dabei werden immer Regeln zwischen einer Benutzergruppe und einem Verbindungsziel angelegt.

LANCOM Trusted Access ist die vertrauenswürdige Network Access Security-Lösung fur Unternehmensnetzwerke. Er ermöglicht einen sicheren und skalierenden Zugriff auf Unternehmensanwendungen für Mitarbeitende im Büro, zu Hause oder unterwegs und schützt damit modernes hybrides Arbeiten von überall und jederzeit. Die LANCOM Trusted Access-Lösung passt sich an steigende Sicherheitsanforderungen in Ihrer Organisation an und ermöglicht sowohl Cloud-managed VPN-Client-Vernetzung für den Zugriff auf ganze Netze als auch den Umstieg auf eine Zero-Trust-Sicherheitsarchitektur für eine umfassende Netzwerksicherheit. Dabei erhalten Benutzer auf Basis granularer Zugriffsrechte ausschließlich Zugangsberechtigung auf Anwendungen, die ihnen zugewiesen wurden (Zero-Trust-Prinzip). Bestehende Systeme zur Verwaltung von Benutzern und Benutzergruppen (Active Directory) lassen sich vollständig in die (LMC) integrieren. Für kleinere Netzwerke bietet die LMC alternativ eine interne Benutzerverwaltung. LANCOM Trusted Access 100% DSGVO-konform und skaliert für Kleinunternehmen genauso wie für sehr große Netzwerke mit mehreren tausend Benutzern.

LTA-Benutzergruppen

Um die LTA-Benutzergruppen von den lokalen / LDAP Gruppen unterscheiden zu können, wurde ein neuer Gruppentyp hinzugefügt: die LTA Gruppen. Ein neues Desktop-Symbol stellt LTA-Benutzergruppen dar.

Symbol / Schaltfläche	Beschreibung
	Erstellen einer LANCOM Trusted Access Benutzergruppe.

Erstellen Sie Desktop-Objekte für LTA-Benutzergruppen (LANCOM Trusted Access). Normalerweise werden diese hier nur angezeigt, da diese über die LANCOM Management Cloud verwaltet werden.

Navigieren Sie zu **Desktop** > **Desktop-Objekte** > **LTA-Gruppen**, um die Liste der derzeit im System angelegten LTA-Benutzergruppenobjekte in der Objektleiste anzuzeigen.

Im Bearbeitungsfenster **LTA-Gruppe** können Sie die folgenden Elemente konfigurieren:

Eingabefeld	Beschreibung
Name	Geben Sie einen Namen für die LTA-Gruppe an.
Beschreibung	Optional: Geben Sie weitere Informationen zur LTA-Gruppe für die interne Verwendung ein.
Gruppen-ID	Die Gruppen-ID, die im Zertifikat des Benutzers verwendet wird.
Tags	Optional: Wählen Sie aus der Drop-down-Liste die Desktop-Tags aus, die Sie der LTA-Gruppe zuweisen möchten.
Farbe	Wählen Sie die Farbe aus, die für dieses Objekt auf dem Desktop verwendet werden soll.

Die Schaltflächen rechts unten im Bearbeitungsfeld hängen davon ab, ob Sie eine neue LTA-Gruppe hinzufügen oder eine bestehende Gruppe bearbeiten. Klicken Sie für eine neu konfigurierte Gruppe auf **Erstellen**, um sie zur Liste der verfügbaren LTA-Gruppen hinzuzufügen, oder auf **Abbrechen**, um Ihre Änderungen zu verwerfen. Zum Bearbeiten einer vorhandenen Gruppe klicken Sie auf **Speichern**, um die neu konfigurierte Gruppe zu speichern, oder auf **Zurücksetzen**, um Ihre Änderungen zu verwerfen. Sie können auf **Schließen** klicken, um das Bearbeitungsfenster zu schließen, solange keine Änderungen darin vorgenommen wurden.

Klicken Sie auf ✔ **Aktivieren** in der Symbolleiste oben im Desktop, um Ihre Konfigurationsänderungen zu übernehmen.

LTA Authentifizierung für IPSec

Bei IPSec-Verbindungen gibt es den neuen Authentifizierungstyp LTA.

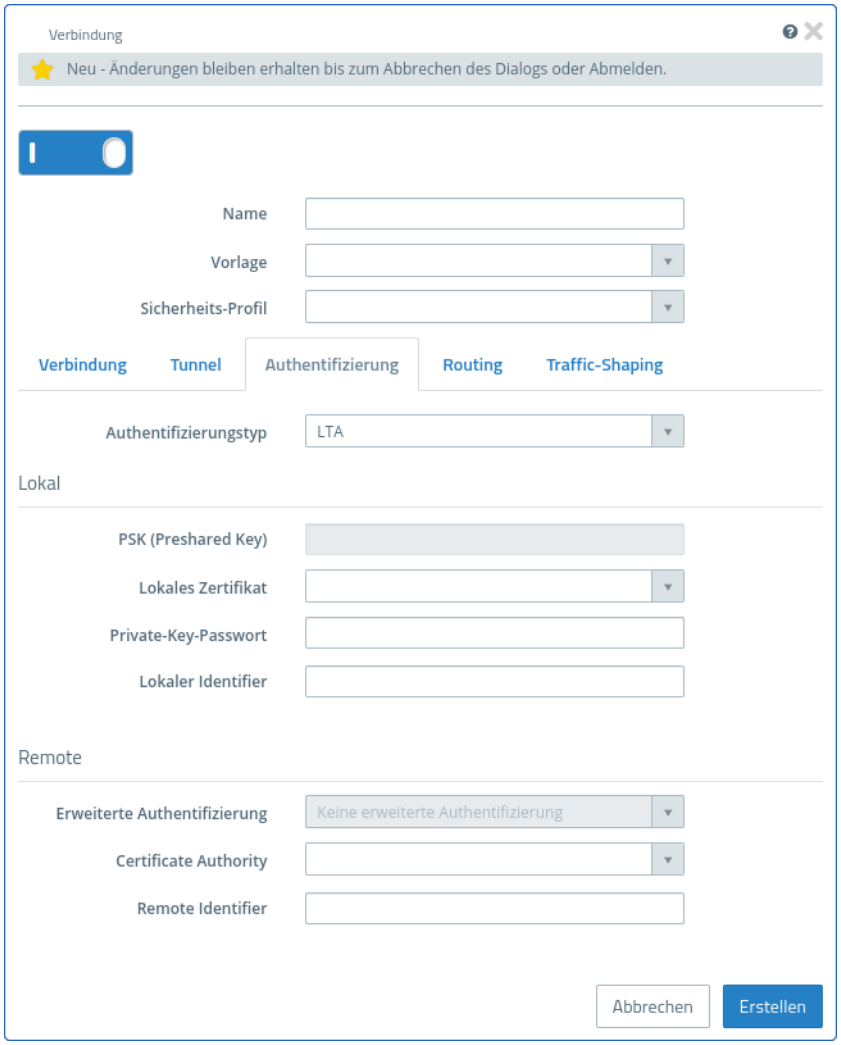

Abbildung 2: VPN > IPsec > Verbindungen

Tabelle 1: Authentifizierung

Eingabefeld	Beschreibung
Authentifizierungstyp	Geben Sie den Authentifizierungstyp an. Mögliche Werte: › … › LTA – bei dem Modus LANCOM Trusted Access wird immer ein Clientzertifikat erwartet und aus diesem Clientzertifikat werden die Gruppen des sich verbindenden Benutzers gelesen, um die dazu passenden Regeln zu aktivieren.

4 Senden von Alarmierungen an die LANCOM Management Cloud

Über die LANCOM Management Cloud kann die Weiterleitung von auf der LANCOM R&S®Unified Firewall generierten Alerts konfiguriert werden. Wenn diese Funktion über die LANCOM Management Cloud aktiviert wurde, dann werden die dort getroffnen Einstellungen im Webclient transparent gemacht.

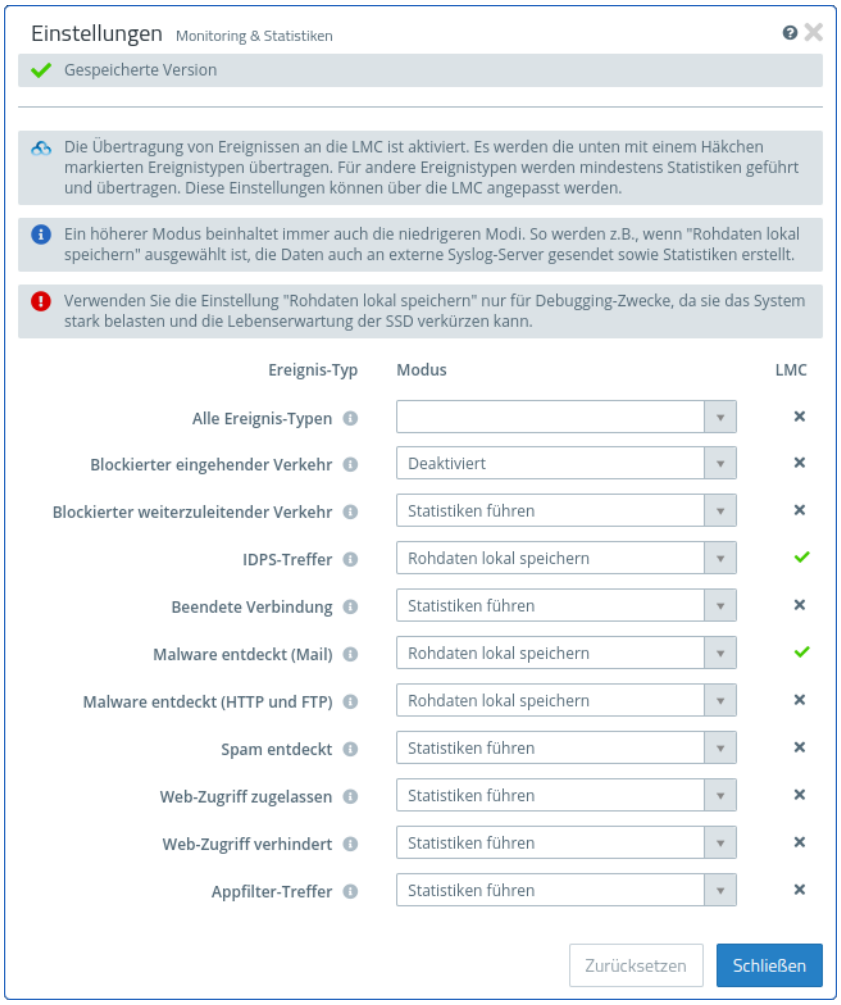

Abbildung 3: Monitoring & Statistiken > Einstellungen

In der Spalte **LMC** wird angezeigt, wenn in der LANCOM Management Cloud die Weiterleitung von generierten Meldungen zu Ereignistypen eingestellt wurde. Alle an die LANCOM Management Cloud gesendeten Ereignistypen werden mit einem grünen Haken dargestellt. Für die Ereignistypen mit einem X werden zwar keine einzelnen Ereignisse übertragen, aber die Anzahl der aufgetretenen Ergeignisse dennoch an die LANCOM Management Cloud gesendet.

Diese Einstellungen lassen sich über die LANCOM R&S®Unified Firewall nicht direkt ändern. Dies ist nur über die LANCOM Management Cloud möglich. Die Einstellungen werden hier nur der Transparenz halber angezeigt.

5 MTU bei Route-Based-IPsec-Verbindungen

Für Route-Based IPsec-Verbindungen kann nun die MTU sowohl bei den Verbindungen als auch bei den Vorlagen eingestellt werden.

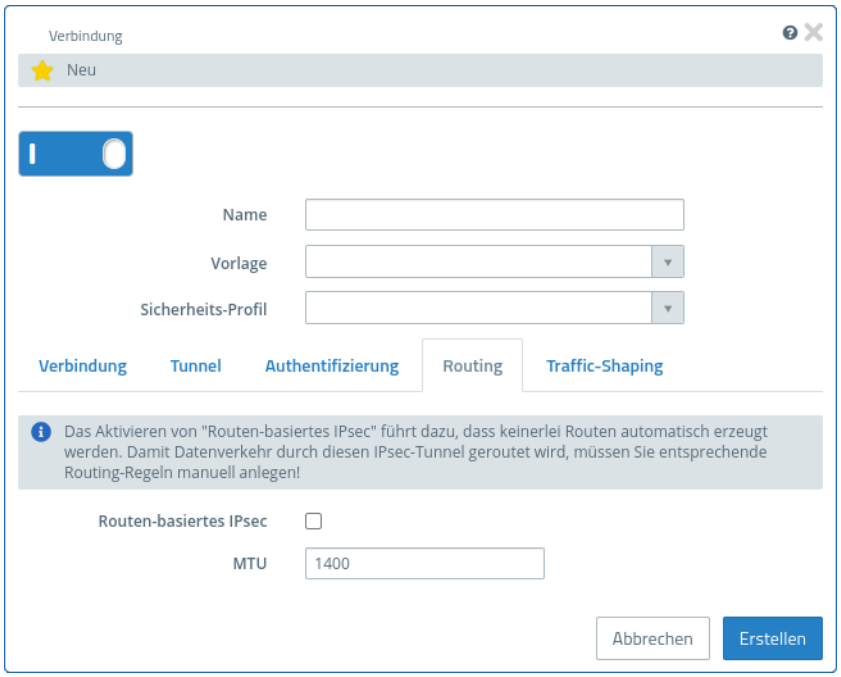

Abbildung 4: VPN > IPsec > Verbindungen / VPN > IPsec > Vorlagen

Tabelle 2: Routing

Eingabefeld	Beschreibung
MTU	Hier können Sie die MTU (Maximum Transmission Unit), also die maximale Größe eines unfragmentierten Datenpakets einstellen. Standardmäßig liegt sie bei 1400.

6 curl-Heartbeats bei WAN-Verbindungen

Neben „ping“ und „tcp_probe“ gibt es nun für WAN-Verbindugnen, für die ein Default Gateway eingerichtet ist, auch die Option „curl“-Heartbeats einzurichten.

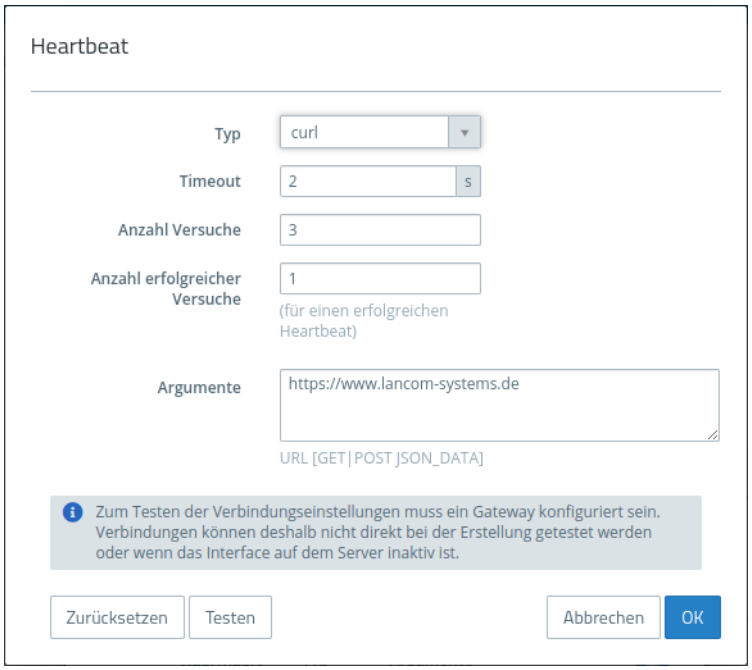

Abbildung 5: Netzwerk > Verbindungen > Netzwerk-Verbindungen > Failover > Heartbeat

Unter Typ können Sie den neuen Modus `curl` einstellen. Dieser Modus erlaubt die HTTP-Request-Methoden GET und POST. Mit POST können an den angegebenen Endpunkt zu sendende Daten im JSON-Format übergeben werden.