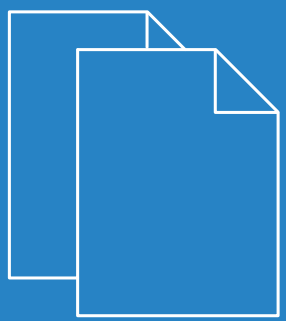
SICHER. **VERNETZT.**

LCOS FX 10.6

Addendum



08/2021

LANCOM Systems

Inhalt

Copyright

LANCOM Systems GmbH

Adenauerstr. 20/B2

52146 Würselen

Deutschland

www.lancom-systems.de

1 Addendum zur LCOS FX-Version 10.6

Dieses Dokument beschreibt die Änderungen und Ergänzungen in der LCOS FX-Version 10.6 gegenüber der vorherigen Version.

2 IDS / IPS und Anti-Virus pro Netzwerk

Ab LCOS FX-Version 10.6 RU3 können einzelne Hosts oder Netze gezielt von der Prüfung durch die IDS / IPS und die Anti-Virus-Funktionen der LANCOM R&S®Unified Firewall ausgenommen werden. Die Einstellungen hierzu werden in den jeweiligen Desktop-Objekten (Host-, Netzwerk- und Host- / Netzwerkgruppen-Objekte) vorgenommen.

Die Einstellungen sehen für Hosts und Netzwerke gleich aus, hier am Beispiel eines Host-Objektes gezeigt:

Abbildung 1: Host-Objekt

Über die unteren beiden Häkchen kann das Objekt explizit von der Prüfung durch das jeweilige Feature ausgenommen werden. Ein Objekt kann auch bereits implizit von der Prüfung ausgeschlossen sein. Das ist der Fall, wenn es in einem Netzbereich liegt, der bereits durch ein übergeordnetes Objekt explizit von der Prüfung ausgenommen wurde. In diesem Fall erscheint ein entsprechender Hinweis unterhalb der Checkbox, der auch die Namen der Objekte aufführt, von denen die Einstellung „geerbt" wurde.

Das Ausnehmen von der Prüfung erfolgt für Host- / Netzwerk-Gruppen auf die gleiche Weise mit einem entsprechenden Häkchen. Die einzelnen Gruppenmitglieder müssen für das Anzeigen eines entsprechenden Hinweises bzgl. der impliziten Ausnahme von den IDS / IPS- und Anti-Virus-Features jedoch einzeln betrachtet werden.

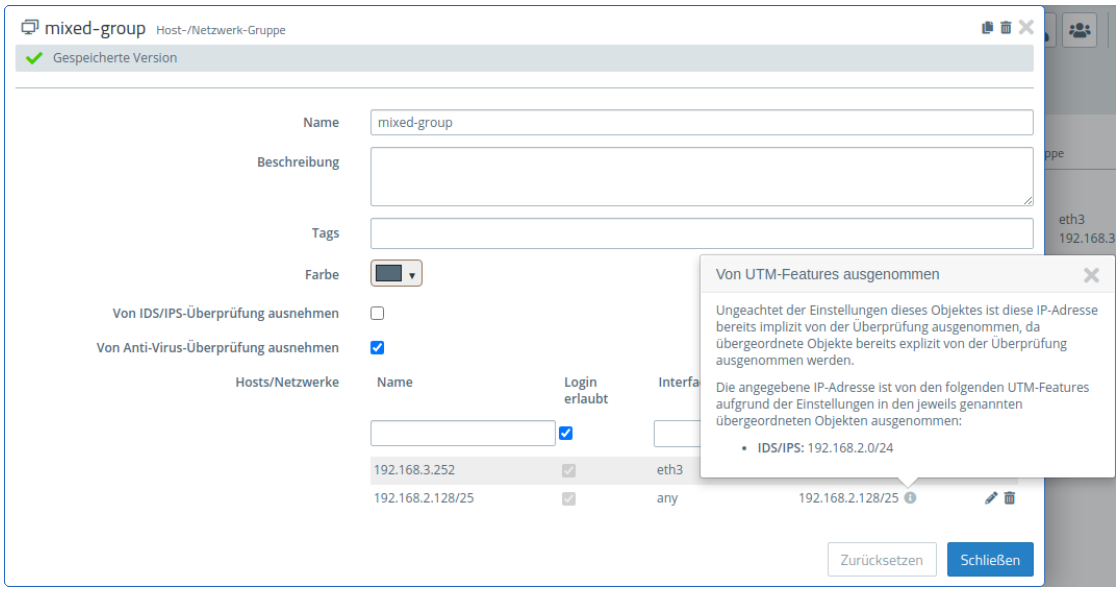


Abbildung 2: Gruppen-Objekt

Ist ein Gruppenmitglied bereits implizit von der Prüfung ausgenommen, so erscheint rechts neben der IP-Adresse ein kleines -Symbol. Ein Klick hierauf öffnet dann ein kleines Popover mit einer Erklärung sowie einer Liste der UTM-Features, von denen das Gruppenmitglied ausgenommen ist, und von welchen übergeordneten Objekten diese Einstellung geerbt wurde.

3 IPsec-Verbindungseinstellungen

Ab LCOS FX-Version 10.6 RU3 haben sich die Remote-Gateway-Einstellungen geändert. Statt nur einem Remote-Gateway kann jetzt eine Liste von Gateways eingetragen werden. Diese Änderung betrifft sowohl die Einstellungen einer IPsec-Verbindung (**VPN** > **IPsec** > **Verbindungen**) als auch die einer Verbindungsvorlage (**VPN** > **IPsec** > **Vorlagen**).

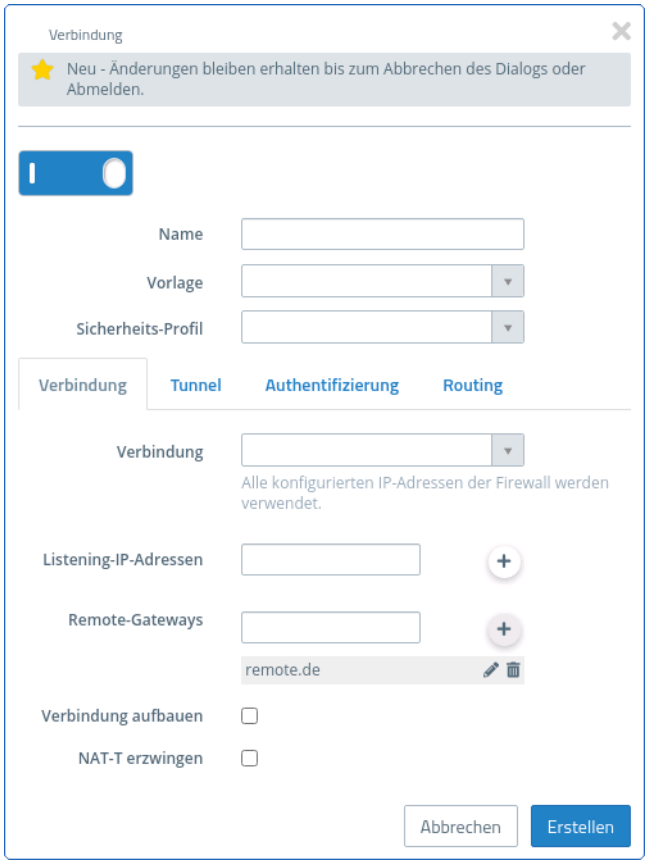


Abbildung 3: IPsec-Verbindung

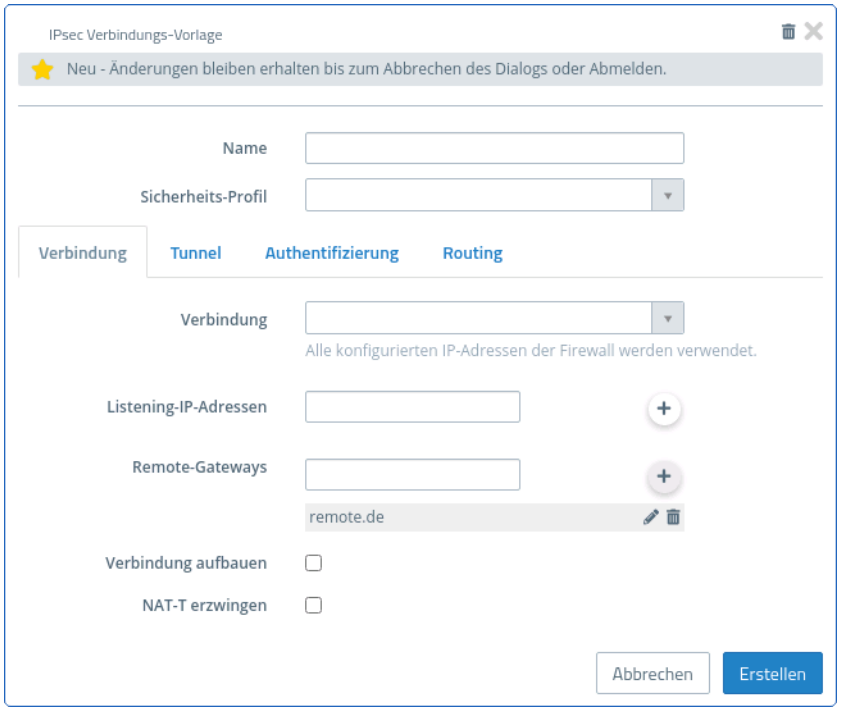
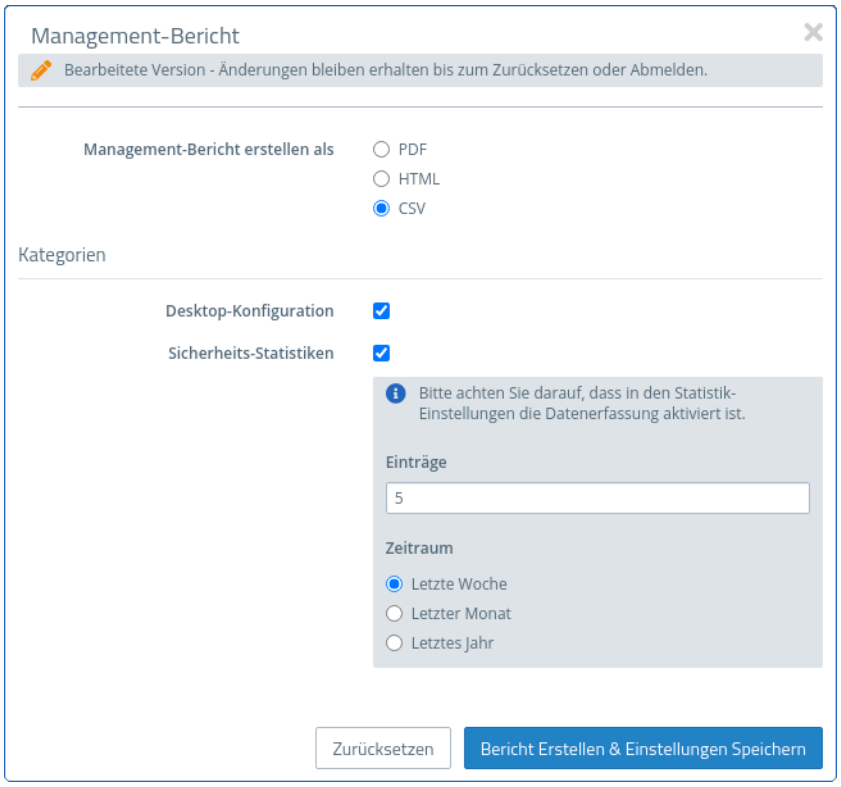


Abbildung 4: IPsec-Verbindungsvorlage

4 Management-Bericht als CSV-Export

Ab LCOS FX-Version 10.6 RU1 kann der Management-Bericht auch im CSV-Format exportiert werden.



Bei dem Format CSV werden die Tabellen als einzelne `csv`-Dateien erstellt und zusammengepackt als ZIP-Datei zum Speichern angeboten. So wird eine eventuelle Weiterverarbeitung der Daten vereinfacht.

5 DNS-Einstellungen

Ab LCOS FX-Version 10.6 verteilen sich die DNS-Einstellungen jetzt unterhalb von **Netzwerk** > **DNS-Einstellungen** auf zwei Menüpunkte. Einen für die globalen Einstellungen (**Allgemeine Einstellungen**), die gelten, wenn keine Netz-spezifischen Einstellungen diese überschreiben. Und einen für die Netz-spezifischen Einstellungen (**Netzwerk-spezifische Einstellungen**), in dem Einstellungen in Abhängigkeit des Quell-Netzes, aus dem DNS-Anfragen stammen, gemacht werden können.

5.1 Allgemeine Einstellungen

Navigieren Sie zu **Netzwerk** > **DNS-Einstellungen** > **Allgemeine Einstellungen**, um die globalen DNS-Einstellungen auf Ihrer LANCOM R&S®Unified Firewall zu konfigurieren.

Normalerweise werden die DNS-Server-Einstellungen von der WAN-Verbindung vorgegeben. Sie sollten die DNS-Server-Einstellungen nur konfigurieren müssen, wenn Sie sie nicht über die WAN-Verbindung beziehen können.

Im Bearbeitungsfenster **Allgemeine Einstellungen** können Sie die folgenden Elemente konfigurieren:

Eingabefeld	Beschreibung
Bezogenene Server	Hier werden die DNS-Server aufgelistet, die über DHCP- und PPP-Verbindungen o. ä. gelernt wurden.
DNS-Server	Diese Tabelle erlaubt die Konfiguration von 1 bis 2 DNS-Servern pro Zone. Eine Zone ist ein bestimmter DNS-Bereich wie „*.company.intern“. Die Standard-Zone „*“ ist die Zone, in die jede DNS-Adresse fällt, die in keine spezifischere Zone fällt. Die „AUTO“-Einstellung ist nur für die Standard-Zone gültig und kann dort dann nicht zusammen mit manuell eingetragenen IP-Adressen verwendet werden, sondern muss alleine stehen. Wird „AUTO“ eingestellt, dann werden an dieser Stelle die oben aufgelisteten, automatisch gelernten DNS-Server genutzt. Die Tabelle kann – mit Ausnahme der Standard-Zone, die immer das letzte Element ist und sich auch nicht löschen lässt – vom Ihnen sortiert werden.
Multicast-DNS-Relay	Aktivieren Sie hier das Multicast-DNS-Relay. Multicast-DNS (mDNS) ist eine Alternative zum herkömmlichen DNS, um Hostnamen in (kleinen) Netzwerken aufzulösen. Dabei wird statt bei einem Server die Namensauflösung anzufragen, eine Anfrage per Multicast an alle durch die Multicast-Adresse erreichbaren Hosts gesendet und verarbeitet. Populäre Implementierungen von mDNS sind Bonjour (Apple) und Avahi (Linux), die das Vernetzen verschiedener Geräte (z.B. Netzwerkdrucker) ermöglichen, ohne vorher irgendwelche Konfigurationsarbeiten durchzuführen.

Wenn Sie diese Einstellungen ändern, klicken Sie zum Speichern Ihrer Änderungen auf **Speichern** oder auf **Zurücksetzen**, um sie zu verwerfen. Klicken Sie ansonsten auf **Schließen**, um das Bearbeitungsfenster zu schließen.

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

5.2 Netzwerk-spezifische Einstellungen

Navigieren Sie zu **Netzwerk** > **DNS-Einstellungen** > **Netzwerk-spezifische Einstellungen**, um in Abhängigkeit des Quellnetzes von DNS-Anfragen alternative Konfigurationen vorzunehmen.

Im Bearbeitungsfenster **Netzwerk-spezifische Einstellungen** können Sie die folgenden Elemente konfigurieren:

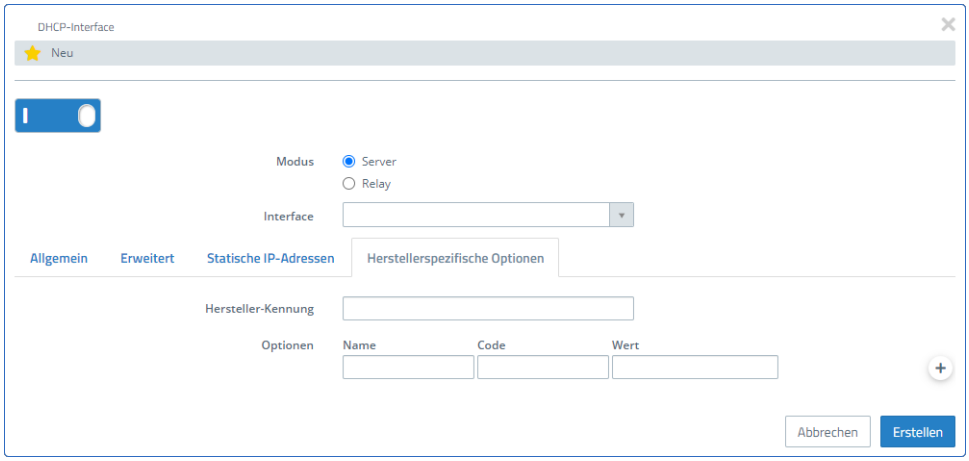
Eingabefeld	Beschreibung
I/0	Ein Schiebeschalter gibt an, ob dieser Einstellungssatz derzeit aktiv (**I**) oder inaktiv (**0**) ist. Mit einem Klick auf den Schiebeschalter können Sie den Status ändern. Ein neuer Einstellungssatz ist standardmäßig aktiviert.
Name	Hier können Sie diesen Netzwerk-spezifischen Einstellungen einen Namen geben.
Quell-Netzwerke	Geben Sie hier eine Liste der Subnetze an, für die dieser Eintrag gelten soll. Zwischen unterschiedlichen Einstellungssätzen müssen die Namen eindeutig sein und die Quell-Netzwerke dürfen nicht mehrfach verwendet werden oder sich überschneiden.
DNS-Server	Diese Tabelle erlaubt die Konfiguration von 1 bis 2 DNS-Servern pro Zone. Eine Zone ist ein bestimmter DNS-Bereich wie „*.company.intern“. Anders als in den globalen Einstellungen ist es hier nicht zwingend notwendig, eine Einstellung für die Standard-Zone "*" zu treffen. Trifft eine DNS-Anfrage für einen Namen ein, der nicht innerhalb einer der hier eingestellten Zonen liegt, dann werden zur Namensauflösung die globalen Einstellungen verwendet. Die „AUTO“-Einstellung kann hier nicht verwendet werden, es müssen immer konkrete DNS-Server-Adressen angegeben werden.
Globale Einstellungen	Die aktuell gültigen globalen Einstellungen werden hier aufgeführt. Die Tabelle kann hier nicht bearbeitet werden und soll nur der Übersicht beim Erstellen von Netz-spezifischen Tabellen dienen.

Wenn Sie diese Einstellungen ändern, klicken Sie zum Speichern Ihrer Änderungen auf **Speichern** oder auf **Zurücksetzen**, um sie zu verwerfen. Klicken Sie ansonsten auf **Schließen**, um das Bearbeitungsfenster zu schließen.

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

6 DHCP-Optionen

Ab LCOS FX-Version 10.6 wurden die DHCP-Einstellungen um die Möglichkeit erweitert, herstellerspezifische Optionen (DHCP Option 43) zu konfigurieren. Dazu wurde in den DHCP-Interface-Einstellungen ein neuer Tab hinzugefügt. Dies wird zum Beispiel von der LANCOM Management Cloud genutzt um LMC-Domain, Projekt-ID und Standort an andere LANCOM Geräte zum Beispiel Access Points zu verteilen.

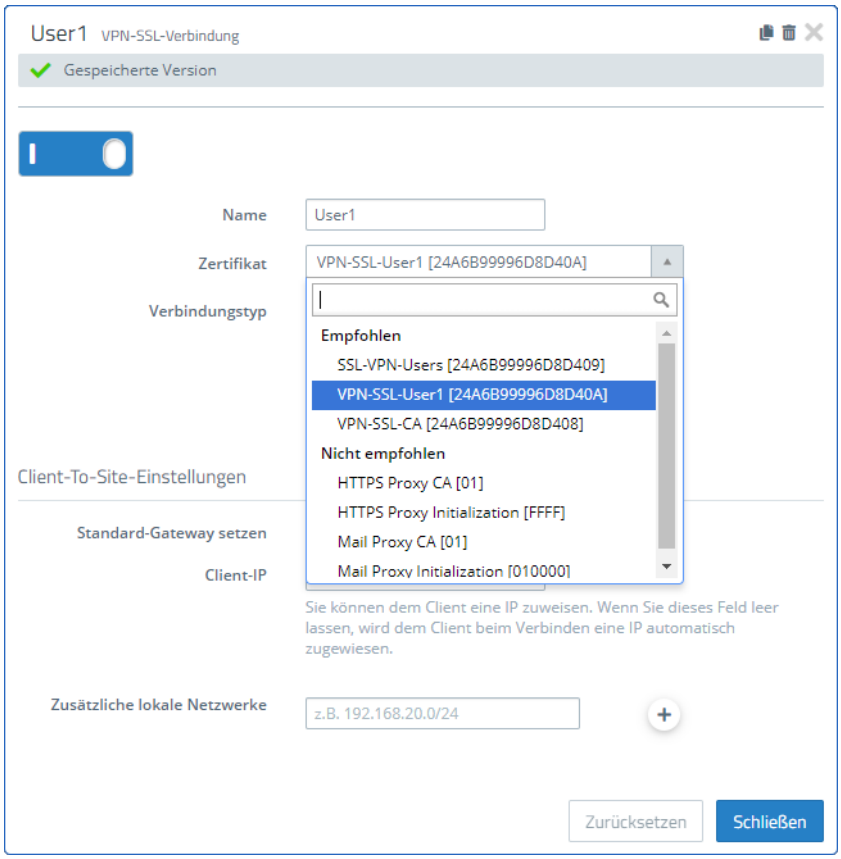


Im Tab Herstellerspezifische Optionen:

Eingabefeld	Beschreibung
Hersteller-Kennung	Hier haben Sie die Möglichkeit herstellerspezifische Optionen (DHCP Option 43) zu konfigurieren. Die Kennung hat eine maximale Länge von 64 Zeichen und darf aus den Zeichen a-z, A-Z, 0-9 und _ bestehen. Dies wird zum Beispiel von der LANCOM Management Cloud genutzt, um LMC-Domain, Projekt-ID und Standort an andere LANCOM Geräte zum Beispiel Access Points zu verteilen.
Optionen	› **Name** Der Name der Option. Dieser hat eine maximale Länge von 64 Zeichen und darf aus den Zeichen a-z, A-Z, 0-9 und _ bestehen. › **Code** Nummer der Option, die an die DHCP-Clients übermittelt werden soll. Die Options-Nummer beschreibt die übermittelte Information, z. B. „43“ für herstellerspezifische Optionen. Eine Liste aller DHCP-Optionen finden Sie im *RFC 2132 – DHCP Options and BOOTP Vendor Extensions* der Internet Engineering Task Force (IETF). › **Wert** In diesem Feld definieren Sie den Inhalt der DHCP-Option. IP-Adressen werden in der üblichen Schreibweise von IPv4-Adressen angegeben, also z. B. als „123.123.123.100“, Integer-Typen werden als normale Dezimalzahlen eingetragen, Strings als einfacher Text. Mehrere Werte in einem Feld werden mit Kommas separiert, also z. B. „123.123.123.100, 123.123.123.200“. Die maximale Länge des Feldes beträgt 64 Zeichen.

7 Empfohlene Zertifikate bei VPN-SSL-Verbindungen

Ab LCOS FX-Version 10.6 werden in den Einstellungen einer VPN-SSL-Verbindung CAs jetzt auch als „Empfohlen" angezeigt und können für eine VPN-SSL-Verbindung verwendet werden.



D.h. mit der Verwendung der CA können nun mehrere Verbindungen exportiert werden, die auf der Firewall nur einmal definiert werden müssen. Dafür kann im Export-Dialog von VPN-SSL-Verbindungen über **Remote-Zertifikat** ein CA-Zertifikat ausgewählt werden.

Im Falle einer CA-Verbindung muss der Benutzer dort ein Zertifikat auswählen, das von der konfigurierten CA signiert wurde. Bei normalen Zertifikats-Verbindungen ist das konfigurierte Zertifikat vorausgewählt und das Feld ist deaktiviert.

Falls zusätzliche lokale Netzwerke an die Clients übertragen werden müssen, so müssen diese im VPN-SSL-Einstellungs-Dialog global konfiguriert werden. Der Hinweis wurde für den Benutzer auch in dem Verbindungsdialog bei den zusätzlichen lokalen Netzwerken hinzugefügt.