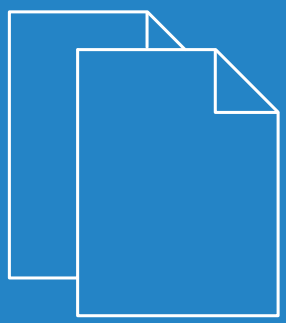
SICHER. **VERNETZT.**

LCOS FX 10.4.0

Addendum



10/2019

LANCOM Systems

Inhalt

Copyright

LANCOM Systems GmbH

Adenauerstr. 20/B2

52146 Würselen

Deutschland

www.lancom-systems.de

1 Addendum zur LCOS FX-Version 10.4.0

Dieses Dokument beschreibt die Änderungen und Ergänzungen in der LCOS FX-Version 10.4.0 gegenüber der vorherigen Version.

2 Getting Started

Ab LCOS FX-Version 10.4.0 steht Ihnen für die Inbetriebnahme Ihrer LANCOM R&S®Unified Firewall ein Assistent zur Verfügung, welcher diesen Prozess erheblich vereinfacht.

2.1 Ersteinrichtung

1. Nehmen Sie das vorinstallierte LANCOM R&S®Unified Firewall-Gerät aus der Verpackung.
2. Verbinden Sie ein Patchkabel mit dem Port mit der Beschriftung **eth1** auf der Frontseite Ihres LANCOM R&S®Unified Firewall-Geräts und mit dem Ethernet-Port Ihres Computers.
3. Verbinden Sie ein Patchkabel mit dem Port mit der Beschriftung **eth0** auf der Frontseite Ihres LANCOM R&S®Unified Firewall-Geräts und mit dem LAN-Port des Geräts (z. B. Ihrem Router, DSL- oder Kabelmodem), welches Sie von Ihrem Provider für den Zugang zum Internet bekommen haben. Stellen Sie sicher, das dieses Gerät eingeschaltet ist.
4. Stellen Sie sicher, dass der Netzwerkadapter Ihres Computer auf „IP-Adresse automatisch konfigurieren" eingestellt ist.
5. Schalten Sie Ihr LANCOM R&S®Unified Firewall-Gerät ein.
6. Starten Sie einen Webbrowser auf Ihrem Computer.
7. Geben Sie in der Adressleiste des Browsers *https://192.168.1.254:3438* ein.
8. Erstellen Sie eine Ausnahme für die Zertifikatwarnung.

   Die LANCOM R&S®Unified Firewall-Loginseite erscheint.
9. Geben Sie auf der Loginseite des LANCOM R&S®Unified Firewall-Webclients `admin` als **Benutzername** und das voreingestellte **Kennwort** `admin` ein.

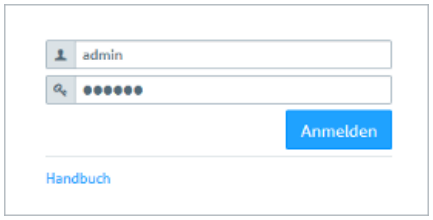


Abbildung 1: Loginseite des LANCOM R&S®Unified Firewall Webclients

10. Klicken Sie auf **Anmelden**.
11. Nach dem ersten Login mit den voreingestellten Anmeldedaten werden Sie vom System aufgefordert, die Endnutzer-Lizenzvereinbarung (EULA) zu akzeptieren und anschließend die folgenden beiden Passwörter zu ändern:
    - Das Passwort für den Benutzer *admin* – Sie benötigen dieses Passwort, um sich beim LANCOM R&S®Unified Firewall-Webclient anzumelden.
    - Das Support-Passwort – Das Support-Passwort ist das Passwort, mit dem der technische Support sich auf Ihrer LANCOM R&S®Unified Firewall anmelden kann. Bewahren Sie es sicher und vor unbefugtem Zugriff geschützt auf.

    Das neue Benutzerpasswort und das Support-Passwort dürfen aus nicht weniger als acht und nicht mehr als 255 Zeichen bestehen. Erlaubt sind lateinische Buchstaben inklusive deutsche Umlaute sowie Zahlen und Sonderzeichen.

Kyrillisch oder andere Schriften nicht. Es müssen Zeichen aus mindestens drei der Kategorien Großbuchstaben, Kleinbuchstaben, Zahlen und Sonderzeichen verwendet werden.

Dieser Schritt ist verpflichtend.

12. Klicken Sie auf **Akzeptieren & Anmelden**, um die neuen Passwörter und die EULA zu akzeptieren.

    Der Setup-Assistent erscheint.

    Mit Ausnahme der Sprachauswahl am Anfang des Setup-Assistenten können Sie den Assistenten jederzeit über die Schaltfläche **Assistent abbrechen** beenden. Nach einem Abbruch des Assistenten können Sie eine manuelle Einrichtung vornehmen, also mit den Schritten *Internetverbindung konfigurieren* und *Internetzugang aktivieren* fortfahren.

    Bis auf wenige Ausnahmen können Sie innerhalb des Setup-Assistenten mit den Schaltflächen **Zurück** und **Weiter** navigieren.

13. Wählen Sie die Sprache für den Setup-Assistenten und den Webclient aus. Sie können die Sprache des Webclient später nach Bedarf jederzeit umschalten.

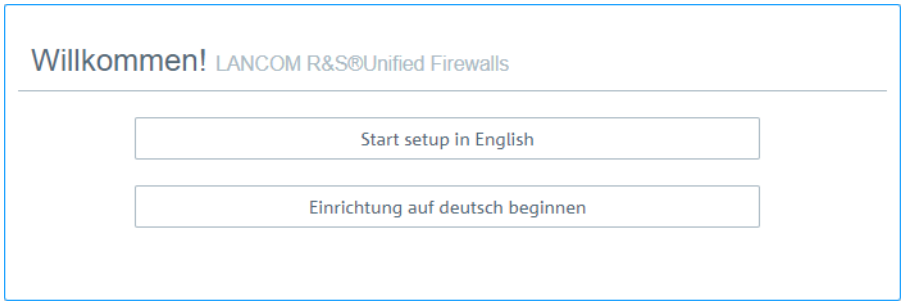


Abbildung 2: Willkommensseite des Setup-Assistenten

14. Wenn Sie die Konfiguration einer vorherigen Installation wiederherstellen wollen, dann klicken Sie auf **Auswählen**, um eine Backup-Datei auszuwählen. Geben Sie das zugehörige Backup-Passwort an. Klicken Sie danach auf **Backup wiederherstellen und neu starten**.

    Anschließend wird der Setup-Assistent beendet, die Konfiguration aus dem Backup wiederhergestellt und die Firewall neu gestartet.

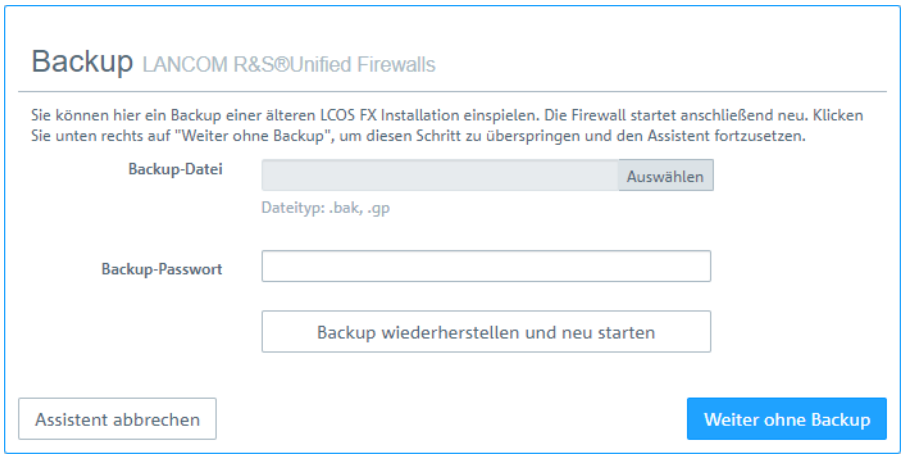


Abbildung 3: Optional eine vorhandene Konfiguration aus einem Backup wiederherstellen

Alternativ fahren Sie für eine Neuinstallation mit **Weiter ohne Backup** fort.

15. Konfigurieren Sie die folgenden allgemeinen Einstellungen der Firewall:

Firewall-Hostname

Geben Sie Ihrer Firewall einen Namen, der als Hostname verwendet wird.

Zeitzone

Die Zeitzone wird mit der momentan im Browser eingestellten Zeitzone vorbelegt. Ändern Sie diese Einstellung bei Bedarf.

Nutzungs-Statistiken senden

Erlauben Sie optional, dass Informationen über Auslastung und Zustand der Firewall aufgezeichnet und an die LANCOM Systems GmbH übermittelt werden. Es werden keine persönlichen Informationen und keine Bestandteile des über die Firewall erfolgten Datenverkehrs übertragen.

Sie köönen diese Einstellung später wieder ändern. Siehe auch *Allgemeine Einstellungen*.

Absturzberichte senden

Erlauben Sie optional, dass im Fehlerfall allgemeine Informationen zum Sytemzustand, zur aktuellen Systemkonfiguration und zum aufgetretenen Fehler an die LANCOM Systems GmbH übertragen werden. Die Daten werden nur zur Fehleranalyse verwendet und anschließend wieder gelöscht. Es erfolgt keine Weitergabe irgendwelcher Daten an Dritte.

Sie können diese Einstellung später wieder ändern. Siehe auch *Allgemeine Einstellungen*.

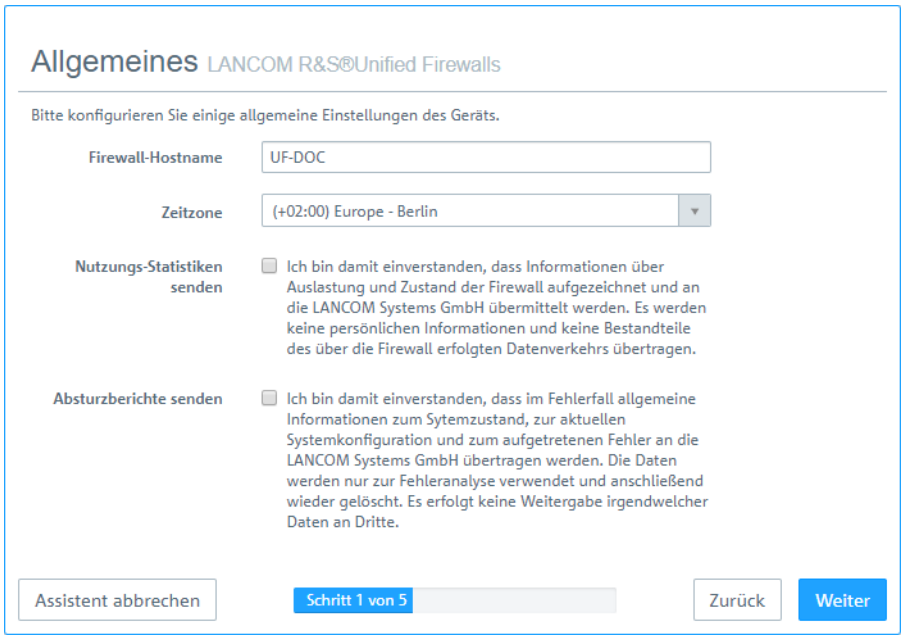


Abbildung 4: Allgemeine Einstellungen der Firewall

16. Selektieren Sie als **Internet-Interface** den Firewall-Port (Standard: **eth0**), mit dem dass Gerät verbunden ist, welches Sie von Ihrem Provider für den Zugang zum Internet bekommen haben. Geben Sie dann Ihre Option für den **Internetzugriff** an:

Abhängig von Ihrer Auswahl können Sie für die Auswahl notwendige Daten konfigurieren.

DHCP

Die IP-Adresse für dieses Interface wird über DHCP bezogen.

Statische Konfiguration

Geben Sie die **IP-Adresse mit Präfix-Länge** (CIDR-Notation), den **Standard-Gateway** und den **DNS-Server** an.

ADSL / SDSL

Geben Sie den **Benutzernamen** und das **Passwort** an, die Sie von Ihrem Internet-Provider erhalten haben.

VDSL

Geben Sie die **VLAN-ID**, den **Benutzernamen** und das **Passwort** an, die Sie von Ihrem Internet-Provider erhalten haben.

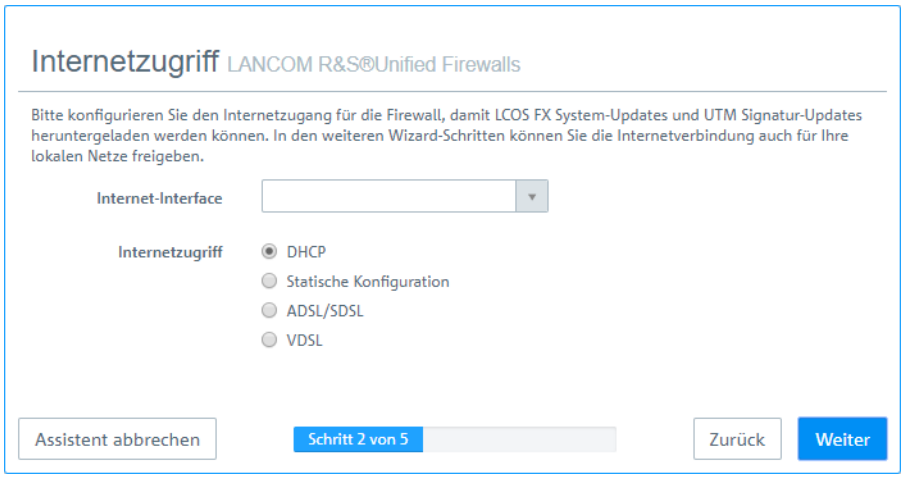


Abbildung 5: Internetzugang

17. Konfigurieren Sie hier das lokale Netzwerk, mit dem die Firewall verbunden ist oder später sein soll. Jede Zeile entspricht einer Netzwerkschnittstelle der Firewall (Spalte **Interface**).

Sie können eine Schnittstelle aktivieren / deaktivieren, je nachdem, ob Sie sie verwenden möchten oder nicht (Spalte **Aktiv**). Die Internet-Schnittstelle kann nicht deaktiviert werden.

Geben Sie im Feld **IP und Präfixlänge** die IP ein, die die Firewall auf dieser Schnittstelle verwenden soll, einschließlich der Präfixlänge (CIDR-Notation). Wenn Sie das Feld leer lassen, hat die Firewall keine IP-Verbindung auf dieser Schnittstelle. In diesem Fall können Sie nicht über diese Schnittstelle auf die Firewall zugreifen und können keinen DHCP-Server oder Web- oder Mail-Zugang für alle Clients zulassen, die über diese Schnittstelle verbunden sind. Jede Schnittstelle sollte ein eigenes Subnetz haben.

Um einen DHCP-Server auf einer Schnittstelle zu aktivieren, aktivieren Sie das Kontrollkästchen **DHCP-Server aktivieren** für eine Schnittstelle. Der DHCP-Bereich hängt von der dieser Schnittstelle zugeordneten Firewall-IP ab und wird auf den größten im Subnetz verfügbaren kontinuierlichen Bereich voreingestellt.

Sie können typischen Internetverkehr (**Web** und **E-Mail**) für Clients zulassen, die mit einer Schnittstelle verbunden sind, indem Sie das entsprechende Kontrollkästchen für eine Schnittstelle aktivieren. **Web** ermöglicht es Clients, sich

über HTTP mit dem Internet zu verbinden. **E-Mail** ermöglicht SMTP-, POP3- und IMAP-Verkehr. Dazu gehören auch die SSL / TLS-Versionen dieser Protokolle.

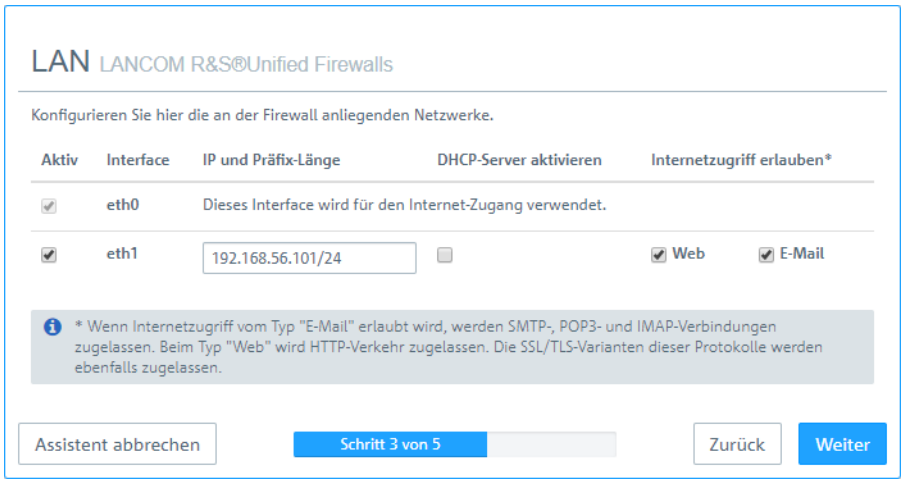


Abbildung 6: Lokale Netzwerke

18. Wählen Sie die Sicherheitsfeatures **Anti-Malware**, **IDS / IPS** und / oder **Content-Filter** aus, die aktivert werden sollen. Abhängig von Ihrem Gerät sind evtl. nicht alle Features verfügbar.

Beim ersten Start nach der Lieferung oder nach einer Neuinstallation läuft die LANCOM R&S®Unified Firewall für 30 Tage als Testversion. Während des Testzeitraums können Sie kein Backup erstellen. Nach Ablauf des Testzeitraums bleibt die Firewall weiterhin mit Ihrer Konfiguration erhalten. Die UTM-Features werden deaktiviert und Sie können keine Änderungen mehr speichern.

Mehr Information hierzu finden Sie unter *Lizenz*.

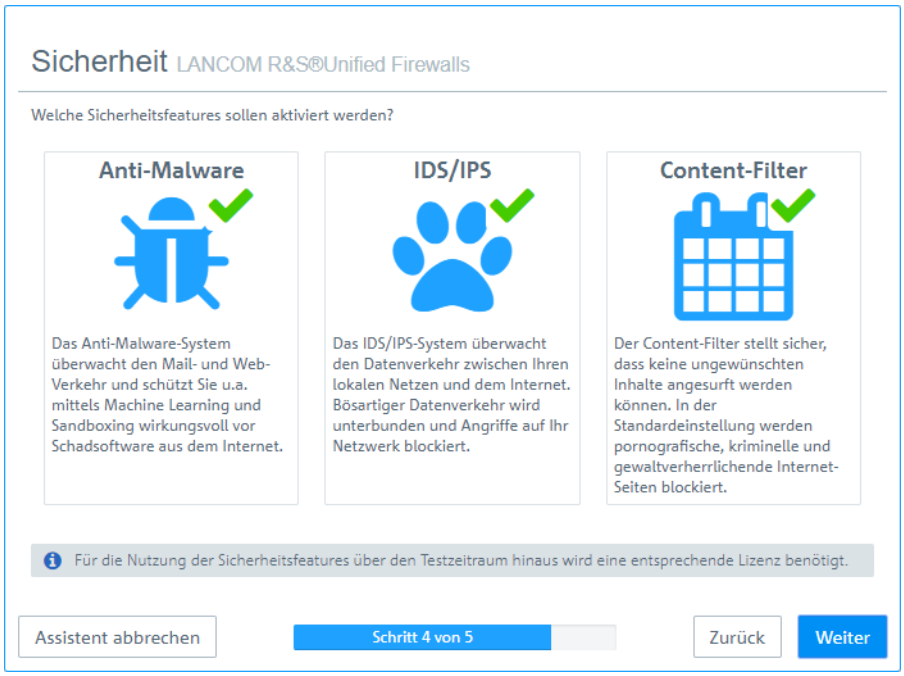


Abbildung 7: Sicherheitsfeatures

19. Hier sehen Sie eine Zusammenfassung der gemachten Einstellungen und können ggfs. zurückgehen, um diese anzupassen. Klicken Sie **Fertigstellen**, wenn alles in Ordnung ist.

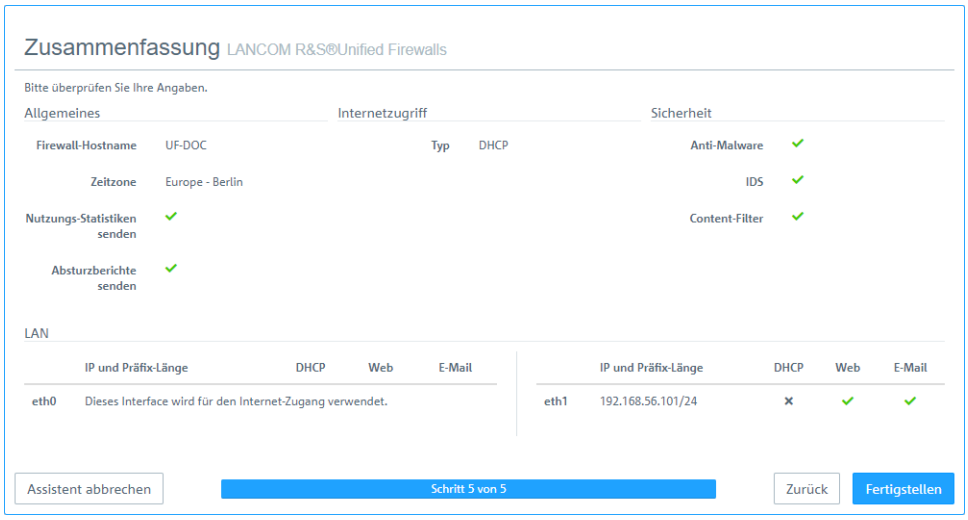


Abbildung 8: Zusammenfassung der gemachten Einstellungen

20. Warten Sie ab bis der Setup-Assistent fertig ist. Nun werden Ihnen die Links angezeigt, über die Sie den Webclient nach Ablauf des Setup-Assistenten erreichen können. Klicken Sie entweder auf einen dieser Links oder auf OK, um zum Webclient zu wechseln.

Wenn Sie das automatisch erzeugt Zertifikat für den Web-Proxy verwenden wollen, dann laden Sie es herunter und rollen es auf Ihre Clients aus.

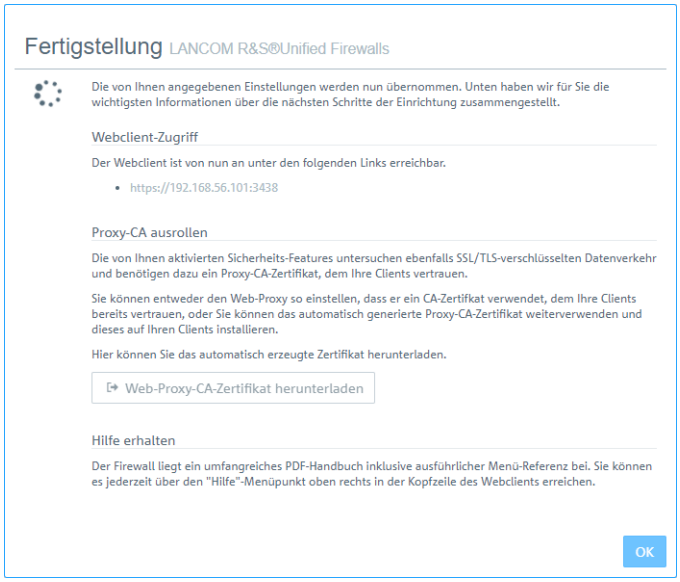


Abbildung 9: Fertigstellung

Falls Sie den Setup-Assistenten erneut verwenden wollen, dann müssen Sie Ihre Firewall auf die Werkseinstellungen zurücksetzen. Siehe hierzu *Kopfzeile*.

3 Werkseinstellungen

Ab LCOS FX-Version 10.4.0 können Sie Ihre LANCOM R&S®Unified Firewall auf die Werkseinstellungen zurücksetzen. Diese neue Option finden Sie n der Kopfzeile. im Menü **System**.

4 Allgemeine Einstellungen

Ab LCOS FX-Version 10.4.0 können Sie einige zentrale Einstellungen in diesem neuen Dialog vornehmen.

Navigieren Sie zu **Firewall** > **Allgemeine Einstellungen**, um ein Bearbeitungsfenster zu öffnen, in dem Sie einige zentrale Einstellungen für Ihre LANCOM R&S®Unified Firewall vornehmen können.

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

Eingabefeld	Beschreibung
Hostname	Hostname der Firewall.
Domain	Domain der Firewall. Falls die Firewall mit einem Active Directory verbunden ist, dann sollte hier die entsprechende Active Directory Domain eingetragen werden.
Nutzungs-Statistiken senden	Informationen über die Auslastung und den Zustand der Firewall aufzeichnen und an die LANCOM Systems GmbH übertragen. Es werden keine persönlichen Informationen und keine Bestandteile des über die Firewall erfolgten Datenverkehrs übertragen.
Absturzberichte senden	Im Fehlerfall allgemeine Informationen zum Sytemzustand, zur aktuellen Systemkonfiguration und zum aufgetretenen Fehler an die LANCOM Systems GmbH übertragen. Die Daten werden nur zur Fehleranalyse verwendet und anschließend wieder gelöscht. Es erfolgt keine Weitergabe irgendwelcher Daten an Dritte.

Wenn Sie Änderungen vorgenommen haben, können Sie diese mit den Schaltflächen unten rechts im Bearbeitungsfenster speichern (**Speichern**) oder verwerfen (**Zurücksetzen**). Andernfalls können Sie das Fenster schließen (**Schließen**).

5 Lizenz herunterladen

Ab LCOS FX-Version 10.4.0 können Sie eine hochgeladene Lizenz auch wieder herunterladen. Dazu einfach die im Lizenzmanager auf dem Tab **Allgemein** neben **Download** als Link angezeigte Lizenzdatei anklicken, sodass der Download der Datei startet.

6 E-Mail-Benachrichtigungen

Ab LCOS FX-Version 10.4.0 können Sie sich von Ihrer LANCOM R&S®Unified Firewall über E-Mails benachrichtigen lassen, wenn bestimmte Systemerreignisse auftreten. Näheres hierzu in den folgenden Abschnitten.

6.1 E-Mail-Einstellungen

Die E-Mail-Einstellungen sind die Voraussetzung für die Nutzung des Benachrichtigungs-Systems. Über dieses können Sie entweder sofort oder regelmäßig in aggregierter Form per E-Mail Nachrichten über bestimmte Benachrichtigungstypen erhalten. Näheres hierzu unter *Benachrichtigungs-Einstellungen* auf Seite 15.

Navigieren Sie zu **Firewall** > **E-Mail-Einstellungen**, um ein Bearbeitungsfenster zu öffnen, in dem Sie die entsprechenden Daten für Absender und Verschlüsselung der Nachrichten konfigurieren können. Optional sind Einstellungen für einen Relay-Server möglich, wenn die E-Mails nicht direkt versendet werden können.

Im Bearbeitungsfenster **E-Mail-Einstellungen** können Sie die folgenden Elemente konfigurieren:

Eingabefeld	Beschreibung
I/**0**	Ein Schiebeschalter gibt an, ob die E-Mail-Einstellungen derzeit aktiv (**I**), oder inaktiv (**0**) sind. Mit einem Klick auf den Schiebeschalter können Sie den Status ändern.
Absender-Adresse	Absender-E-Mail-Adresse des Firewall-Systems.
Verbindungssicherheit	Wählen Sie eine der möglichen Optionen `Keine`, `TLS` oder `StartTLS`.
Remote-Zertifikat verifizieren	Falls dieses angegeben wird, dann verifiziert die Firewall das Zertifikat des Zielservers bzw. Relays.
S/MIME-Zertifikat	Falls dieses angegeben wird, dann verschlüsselt die Firewall alle ausgehenden E-Mails mit dem Public Key des gewählten Zertifikats.

Im Tab **Relay** können Sie Vorgaben für die folgenden Elemente konfigurieren:

Eingabefeld	Beschreibung
Server	Adresse des E-Mail-Servers.
Port	Port des E-Mail-Servers.
Benutzername	Name, mit dem die Firewall sich beim E-Mail-Server anmeldet.
Passwort	Passwort, mit dem die Firewall sich beim E-Mail-Server anmeldet.

Um die vorgenommenen Einstellungen zu testen, können Sie über die Schaltfläche **Test-Mail versenden** eine E-Mail versenden. Es wird ein Dialog geöffnet, in dem Sie eine **Empfänger-Adresse** angeben können und dann über die Schaltfläche **Versenden** diese abschicken.

Beachten Sie, dass, falls ein Relay Server verwendet wird, die darauffolgende Status-Nachricht nur Auskunft darüber gibt, ob die E-Mail vom Relay Server akzeptiert wurde. Kann der Relay Server die Nachricht nicht zustellen, ist das nur auf dem Relay Server zu sehen.

Wenn Sie Änderungen vorgenommen haben, können Sie diese mit den Schaltflächen unten rechts im Bearbeitungsfenster speichern (**Speichern**) oder verwerfen (**Zurücksetzen**). Andernfalls können Sie das Fenster schließen (**Schließen**).

6.2 Benachrichtigungs-Einstellungen

Über das Benachrichtigungs-System können Sie entweder sofort oder regelmäßig in aggregierter Form per E-Mail Nachrichten über bestimmte Benachrichtigungstypen erhalten. Voraussetzung hierfür ist eine aktive E-Mail-Funktion, in der zumindest ein Absender eingestellt ist. Zur Absicherung sind die optionalen Einstellungen **Remote-Zertifikat verifizieren** für die Sicherstellung der korrekten Gegenstelle für den E-Mail-Empfang und **S/MIME-Zertifikat** zur Verschlüsselung der ausgehenden Mail. Näheres hierzu unter *E-Mail-Einstellungen* auf Seite 14

Navigieren Sie zu **Monitoring & Statistiken** > **Benachrichtigungs-Einstellungen**, um ein Bearbeitungsfenster zu öffnen, in dem Sie die folgenden Elemente konfigurieren können:

Tabelle 1: Allgemein

Eingabefeld	Beschreibung
I/**0**	Ein Schiebeschalter gibt an, ob die Benachrichtigungs-Einstellungen derzeit aktiv (**I**), oder inaktiv (**0**) sind. Mit einem Klick auf den Schiebeschalter können Sie den Status ändern.
Benachrichtigungssprache	Stellen Sie die in den Benachrichtigungsmails verwendete Sprache ein. Beim ersten Öffnen des Dialogs wird die für den Webclient eingestellte Sprache verwendet.
Betreff-Vorlage	Legen Sie den Betreff der Benachrichtigungsmail fest.
Empfänger	Liste an Empfänger-Adressen, an die alle Benachrichtigungen verschickt werden. Klicken Sie rechts auf ⊕, um Ihren Eintrag zur Liste hinzuzufügen.

Im Bereich **Aggregierte Benachrichtigungen** können Sie die folgenden Elemente konfigurieren:

Eingabefeld	Beschreibung
Aggregations-Intervall	Die aufgezeichneten Ereignisse werden gesammelt und in einem festgelegten Intervall zusammengefasst als Mail verschickt. Geben Sie hier die Zeitdauer in Minuten an, in der die Ereignisse gesammelt werden, bevor sie als eine Nachricht verschickt werden.
Max. Anzahl Benachrichtigungen pro Mail	Hier legen Sie fest, wie viele Ereignisse in einer Mail zusammengefasst werden. Dies bestimmt somit, wie viele Mails nach Ablauf eines Aggregations-Intervalls auf einmal verschickt werden. Gleichzeitig wird dadurch die maximale Größe der E-Mail begrenzt. ⓘ Beachten Sie ggfs. vorhandene Spam-Richtlinien des Empfängers.

Im Bereich **Sofort-Benachrichtigungen** können Sie die folgenden Elemente konfigurieren:

Eingabefeld	Beschreibung
Max. Anzahl Mails pro Stunde	Wenn ein Ereignis auftritt, für das als Benachrichtigungstyp **Sofort** eingestellt wurde, dann wird sofort eine Mail an die Empfänger verschickt. Abhängig von den Einstellungen im Benachrichtigungstypen-Bereich und den auftretenden Ereignissen könnten viele Mails in kurzer Zeit verschickt werden, die dazu führen, dass diese Mails wegen Nicht-Einhaltung von Richtlinien der Provider auf Empfängerseite blockiert werden. Um dieses zu vermeiden, können Sie hier die maximale Anzahl der verschickten Sofort-Benachrichtigungen pro Stunde begrenzen. ⓘ Alle Sofort-Benachrichtigungen werden auch in der nächsten aggregierten E-Mail verschickt.

Im Bereich **Benachrichtigungstypen** können Sie die folgenden Elemente konfigurieren:

Eingabefeld	Beschreibung
Filtern	Die angezeigten Benachrichtigungsfelder können nach Name und gesetztem Wert gefiltert werden.

Eingabefeld	Beschreibung
Für alle ausgewählten Benachrichtigungen setzen	Alle momentan angezeigten Felder für Benachrichtigungen werden auf den hier eingestellen Wert gesetzt. Um z.B. alle Felder für IPsec auf den **Sofort** einzustellen, geben Sie bei **Filtern** „ipsec“ ein und können dann hier alle IPsec betreffenden Benachrichtigungsfelder auf **Sofort** einstellen.
Erwarteter System-Neustart	Benachrichtigung, wenn das System erwartet neu gestartet wird.
Unerwarteter System-Neustart	Benachrichtigung, wenn das System unerwartet neu gestartet wird.
HA-Rollenwechsel	Benachrichtigung, wenn ein Rollenwechsel in der Hochverfügbarkeit durchgeführt wird.
Internet-Verbindung offline	Benachrichtigung, wenn eine Internet-Verbindung getrennt wird.
Backup-Internet-Verbindung aktiviert	Benachrichtigung, wenn die Standard-Internet-Verbindung durch die Backup-Verbindung ersetzt wird.
Internet-Verbindung online	Benachrichtigung, wenn eine Verbindung zum Internet hergestellt wird.
Standard-Internet-Verbindung reaktiviert	Benachrichtigung, wenn wieder die Standard-Internet-Verbindung genutzt wird.
IPsec Site-to-Site-Verbindung online	Benachrichtigung, wenn eine IPsec Site-to-Site-Verbindung hergestellt wird.
IPsec Site-to-Site-Verbindung offline	Benachrichtigung, wenn eine IPsec Site-to-Site-Verbindung getrennt wird.

Wenn Sie Änderungen vorgenommen haben, können Sie diese mit den Schaltflächen unten rechts im Bearbeitungsfenster speichern (**Speichern**) oder verwerfen (**Zurücksetzen**). Andernfalls können Sie das Fenster schließen (**Schließen**).

7 LANCOM Management Cloud (LMC)

Ab LCOS FX-Version 10.4.0 können Sie Ihre LANCOM R&S®Unified Firewall über die LMC verwalten.

Symbol / Schaltfläche	Beschreibung
	Hiermit werden alle Objekte und Einstellungen gekennzeichnet, die durch die LANCOM Management Cloud (LMC) verwaltet werden. Diese können mit dem Webclient eingesehen, aber nicht bearbeitet werden. Durch die LMC verwaltete Objekte lassen sich nicht referenzieren. Somit kann z.B. ein durch die LMC erstelltes Application Filter-Profil nicht in einer selbst erstellten Desktop-Verbindung verwendet werden.

7.1 LANCOM Management Cloud-Einstellungen

Hier finden Sie die Einstellungen für die Konfiguration und das Monitoring Ihres Gerätes durch die LANCOM Management Cloud (LMC).

Navigieren Sie zu **Firewall** > **LMC-Einstellungen**, um ein Bearbeitungsfenster zu öffnen, in dem Sie die Einstellungen für die LMC anzeigen und anpassen können.

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

Eingabefeld	Beschreibung
I/0	Ein Schiebeschalter gibt an, ob die Verwaltung der Firewall über die LANCOM Management Cloud aktiv (**I**) oder inaktiv (**0**) ist. Mit einem Klick auf den Schiebeschalter ändern Sie den Status dieser Option.
LMC-Domain	Geben Sie hier den Domain-Namen der LMC an. Standardmäßig ist die Domain für den ersten Verbindungsaufbau mit der Public LMC eingetragen. Möchten Sie Ihr Gerät von einer eigenen Management Cloud verwalten lassen („Private Cloud" oder „on premise installation"), tragen Sie bitte die entsprechende LMC-Domain ein.
Aktivierungscode	Alternativ zur Eingabe der Seriennummer und der dem Gerät beiliegenden Cloud-PIN kann ein Gerät auch über einen Aktivierungscode einem Projekt in der LMC zugewiesen werden. Klicken Sie dazu in der LMC unter **Geräte** auf **Aktivierungscodes**, danach auf **Aktivierungscode erstellen**. Sie können dort einen zeitlich beschränkt gültigen Aktivierungscode generieren. Dieser kann innerhalb des Gültigkeitszeitraums auf beliebig vielen LANCOM Geräten zur Aktivierung, also zur Übernahme in die LMC, genutzt werden.

8 VPN

Ab LCOS FX-Version 10.4.0 wurde die Menüstruktur für VPN und alle IPsec betreffenden Dialoge durch eine neue Implementation dieses Features geändert. Näheres hierzu in den folgenden Abschnitten.

8.1 VPN

Mit den Einstellungen unter **VPN** können Sie Ihre LANCOM R&S®Unified Firewall für die Verwendung als Virtual Private Network-Server konfigurieren, um Client-to-Site (C2S)-VPN-Verbindungen zur Verfügung zu stellen. So können Computer an einem anderen Ort mittels IPsec und VPN-SSL sicher auf Ressourcen im lokalen Netzwerk zugreifen. Durch ein *Site-to-Site* (S2S) VPN-Gateway kann über das Internet mittels IPsec und VPN-SSL ein sicherer Kommunikationskanal zwischen zwei Remote-Netzwerken aufgebaut werden.

Client-to-Site VPN-Verbindungen

Durch eine Client-to-Site VPN-Verbindung kann das Unternehmensnetzwerk von außen erreicht werden. Die Authentifizierung erfolgt entweder über IPsec mit ausgestellten Zertifikaten, mittels eines so genannten PSK (Pre-Shared Key) oder über VPN-SSL mit Zertifikaten.

Client-to-Site-Verbindungen über IPsec und VPN-SSL können abhängig von den Client-Einstellungen in einem von zwei Modi betrieben werden:

- Im *Split-Tunnel-Modus* wird nur die Kommunikation zwischen dem Client und dem internen Netzwerk (z. B. einem Unternehmensnetzwerk) durch die Firewall geleitet. Clients können Geräte im internen Netzwerk über den Tunnel erreichen. Für andere Ziele (wie das Internet) vorgesehene Pakete werden nicht durch die LANCOM R&S®Unified Firewall geroutet.

  Beispiel: Ein Benutzer wählt sich mithilfe eines VPN-Software-Clients per Fernzugriff aus dem Drahtlosnetzwerk eines Hotels in ein Unternehmensnetzwerk ein. Durch Split Tunneling kann der Benutzer sich über die VPN-Verbindung mit Dateiservern, Datenbankenservern, Mailservern und anderen Diensten im Unternehmensnetzwerk verbinden. Verbindet sich der Benutzer mit Internetressourcen (Websites, FTP-Seiten etc.), wird die Verbindungsanfrage direkt über das Gateway des Hotelnetzwerks abgesendet.

- Im *Full-Tunnel-Modus* wird der gesamte Datenverkehr zurück zu Ihrer LANCOM R&S®Unified Firewall geleitet, einschließlich der Kommunikation mit Internetseiten.

  Full Tunneling erlaubt es dem Benutzer beispielsweise nicht, über Hotelnetzwerke direkt auf das Internet zuzugreifen. Jeglicher Datenverkehr, der vom Client ausgesendet wird, während die VPN-Verbindung aktiv ist, wird an die Firewall gesendet.

C2S-Verbindungen über IPsec werden mithilfe eines gewöhnlichen VPN-Clients hergestellt, z. B. dem LANCOM Advanced VPN Client. Weitere Informationen finden Sie unter *IPsec-Verbindungs-Einstellungen* auf Seite 25.

VPN-SSL C2S-Verbindungen werden mithilfe eines gewöhnlichen VPN-Clients hergestellt. Weitere Informationen finden Sie unter *VPN-SSL-Verbindungseinstellungen* auf Seite 39.

Site-to-Site VPN-Verbindungen

Bei einer Site-to-Site-Verbindung werden zwei Standorte über einen verschlüsselten Tunnel miteinander zu einem virtuellen Netzwerk verbunden und tauschen durch diesen Tunnel Daten aus. Die beiden Standorte können feste IP-Adressen

haben. Die Authentifizierung erfolgt entweder über IPsec mit ausgestellten Zertifikaten, mittels eines so genannten PSK (Pre-Shared Key) oder über VPN-SSL mit Zertifikaten.

IPsec

IPsec (Internet Protocol Security) ist ein Satz von Protokollen, der auf Ebene der Vermittlungsschicht oder der Sicherungsschicht arbeitet und den Austausch von Paketen über nicht vertrauenswürdige Netzwerke (bspw. das Internet) sichert, indem er jedes IP-Paket einer Kommunikationssitzung authentifiziert und verschlüsselt. IPsec erfüllt die höchsten Sicherheitsanforderungen.

VPN-SSL

VPN über SSL bietet eine schnelle und sichere Möglichkeit, eine Roadwarrior-Verbindung einzurichten. Der größte Vorteil an VPN-SSL ist, dass der gesamte Datenverkehr über einen TCP- oder UDP-Port läuft und im Gegensatz zu IPsec keine weiteren speziellen Protokolle benötigt werden.

Stellen Sie vor der Einrichtung von VPN-Verbindungen sicher, dass Sie die notwendigen Zertifikate installiert haben, wie unter *Zertifikatsverwaltung* beschrieben.

8.1.1 IPsec

Die IPsec-Protokollsuite (Internet Protocol Security) arbeitet auf der Ebene der Vermittlungsschicht und nutzt die Authentifizierung und Verschlüsselung von IP-Paketen, um die Kommunikation in nicht vertrauenswürdigen Netzwerken abzusichern.

Für eine Site-to-Site-Verbindung über IPsec benötigen Sie zwei VPN-IPsec-fähige Server. Für eine Client-to-Site-Verbindung benötigen Sie separate Client-Software.

Ihre LANCOM R&S®Unified Firewall ist in der Lage, mithilfe der IPsec-Protokollsuite sichere Verbindungen aufzubauen und zu nutzen. Ermöglicht wird dies durch ESP im Tunnel-Modus. Der Schlüsselaustausch kann mithilfe von Version 1 des IKE-Protokolls oder des neueren IKEv2 erfolgen. Nach Wahl werden Pre-shared Keys oder Zertifikate nach dem X.509-Standard verwendet. Mit IKEv1 ist auch eine Authentifizierung über XAUTH möglich. Beu IKEv2 gibt es die zusätzliche Authentifizierungsmöglichkeit über EAP.

IPsec-Einstellungen

Unter **VPN** > **IPsec** > **IPsec-Einstellungen** können Sie IPsec aktivieren und die Einstellungen konfigurieren:

Tabelle 2: Allgemein

Eingabefeld	Beschreibung
I/0	Ein Schiebeschalter gibt an, ob IPSec aktiv (**I**) oder inaktiv (**0**) ist. Mit einem Klick auf den Schiebeschalter ändern Sie den Status dieser Option.
Ausgenommene Interfaces	Auswahlliste, in der Interfaces ausgewählt werden können, die nicht vom IPsec-Dienst verwendet werden sollen. Wenn hier nichts eingetragen ist, dann werden alle Interfaces auf dem System ausgenommen – auch solche die neu erstellt oder automatisch erzeugt werden. Normalerweise werden ausgenomme Interfaces und die ausgenommenen IP-Adressen benötigt, wenn der gesamte Traffic über einen IPsec-Tunnel in die Zentrale geschickt wird. In einem solchen Fall muss man aufpassen, dass die lokalen Netze weiter erreichbar bleiben. Standardmäßig hat IPsec eine höhere Priorität als normale Routen und somit würden selbst Pakete, die für lokale Netze gedacht sind, stattdessen in den VPN-Tunnel geschickt. Im Normalfall bleiben also durch die Voreinstellung, alle lokalen Interfaces auszunehmen, die lokalen Netze immer erreichbar.
Ausgenommene IP-Adressen	Tragen Sie hier IP-Adressen im CIDR-Format ein. Pakete zu diesen Netzen werden unter keinen Umständen in einen Tunnel weitergeleitet, selbst dann nicht, wenn ein Tunnel für die Zieladresse konfiguriert ist.

Eingabefeld	Beschreibung
	Klicken Sie rechts auf ⊕, um Ihren Eintrag zur Liste der IP-Adressen hinzuzufügen.
Proxy-ARP	Ist diese Option aktiv, dann antwortet die Firewall auf ARP-Anfragen aus lokalen Netzen für virtuelle IP-Adressen, die an IPsec-Clients vergeben wurden, mit der eigenen MAC-Adresse.

Tabelle 3: DHCP-Server

Eingabefeld	Beschreibung
Aktiv	IPsec kann einen DHCP-Server verwenden, um den verbundenen IPsec-Clients virtuelle IP-Adressen zuzuweisen. Hier können Sie diese Funktion aktiveren. Zur Verwendung wählen Sie in einer IPsec-Verbindung bei **Virtueller IP-Pool** die Option **DHCP Virtual-IP pool** aus.
IP-Adresse	Geben Sie hier die IP-Adresse des zu verwendenden DHCP-Servers ein. Dies kann entweder die Adresse eines DHCP-Servers sein oder eine Broadcast-Adresse eines Netzwerks.

Tabelle 4: RADIUS-Server

Eingabefeld	Beschreibung
Aktiv	IPsec kann in Verbindung mit EAP oder XAUTH die Benutzerverwaltung eines RADIUS-Servers verwenden, um die Verbindung zu authentifizieren. Ausserdem können auch IP-Adressen vom RADIUS-Server an IPsec-Clients zugewiesen werden. Dafür wählen Sie in einer IPsec-Verbindung bei **Virtueller IP-Pool** die Option **RADIUS Virtual-IP pool** aus. Hier können Sie diese Funktion aktiveren.
IP-Adresse	IP-Adresse des RADIUS-Servers.
Port	Port des RADIUS-Servers.
Passwort	Passwort für den Zugriff auf den Radius-Server.

Wenn Sie Änderungen vorgenommen haben, können Sie diese mit den Schaltflächen unten rechts im Bearbeitungsfenster speichern (**Speichern**) oder verwerfen (**Zurücksetzen**). Andernfalls können Sie das Fenster schließen (**Schließen**).

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

Sicherheits-Profile

Unter **VPN** > **IPsec** > **Sicherheits-Profile** finden Sie eine Liste von vordefinierten Profilen, die Sie mit selbst erstellten Profilen erweitern können.

Die vordefinierten Profile können weder bearbeitet noch gelöscht werden.

Werden verwendete Sicherheits-Profile geändert, können in der erweiterten Listbar alle zugehörigen Verbindungen neugestartet werden. Sicherheits-Profile werden in Vorlagen und Verbindungen gewählt.

Klicken Sie auf ⊕, um ein neues Sicherheitsprofil hinzuzufügen.

Tabelle 5: Allgemeine Einstellungen

Eingabefeld	Beschreibung
Name	Geben Sie diesem Sicherheitsprofil einen aussagekräftigen Namen.
Verwendet in	Zeigt an, in welchen IPsec-Verbindungen dieses Profil aktuell verwendet wird.

Eingabefeld	Beschreibung
Datenkomprimierung	Wenn man hier Datenkomprimierung wählt, dann wird diese für alle Verbindungen aktiviert, die dieses Profil verwenden. Man spart dadurch zwar Bandbreite, erhöht aber auch die CPU-Last. Wenn Sie Datenkomprimierung aktivieren, dann muss diese auch auf der Gegenstelle aktiviert sein.

ISAKMP (IKE)

In diesem Tab können Sicherheits-Einstellungen für die IKE-Phase definiert werden. IKE definiert, wie Sicherheitsparameter vereinbart und gemeinsame Schlüssel ausgetauscht werden

Tabelle 6: ISAKMP (IKE)

Eingabefeld	Beschreibung
IKE-Version	Wählen Sie IKEv1 oder IKEv2
Verschlüsselungsalgorithmen	Wählen Sie aus der Liste der verfügbaren Verschlüsselungsalgorithmen diejenigen aus, die Sie verwenden wollen.
Authentifizierungsalgorithmen	Wählen Sie aus der Liste der verfügbaren Authentifizierungsalgorithmen diejenigen aus, die Sie verwenden wollen.
DH-Gruppen	Wählen Sie aus der Liste der verfügbaren Diffie-Hellmann-Gruppen diejenigen aus, die Sie verwenden wollen.
SA-Lebensdauer	Geben Sie die gewünschte SA-Lebensdauer in Sekunden an.
Mobile IKE (nur IKEv2)	Diese nur für IKEv2 verfügbare Option erlaubt das Wechseln der IP-Adressen ohne Verbindungsabbruch.

Die Verschlüsselungsalgorithmen, Authentifizierungsalgorithmen und DH-Gruppen, die hier definier werden, werden beim Aufbau der IPsec-Verbindung verwendet, um eine Verschlüsselungs-Authentifizierungs-Kombination mit der Gegenstelle auszuhandeln. Je mehr Einträge hier definiert werden, desto höher sind die Kombinationsmöglichkeiten.

Die Anzahl der Kombinationsmöglichkeiten ist bei Verwendung von IKEv1 auf etwas über 200 begrenzt. Bei IKEv2 gibt es keine Beschränkung.

IPsec (ESP)

Encapsulating Security Payload (ESP) stellt Mechanismen zur Sicherstellung der Authentizität, Integrität und Vertraulichkeit der übertragenen IP-Pakete bereit. Diese Einstellungen bestimmen somit die Verschlüsselungs- und Authentifizierungsalgorithmen der eigentlichen IP-Pakete.

Tabelle 7: IPsec (ESP)

Eingabefeld	Beschreibung
Verschlüsselungsalgorithmen	Wählen Sie aus der Liste der verfügbaren Verschlüsselungsalgorithmen diejenigen aus, die Sie verwenden wollen.
Authentifizierungsalgorithmen	Wählen Sie aus der Liste der verfügbaren Authentifizierungsalgorithmen diejenigen aus, die Sie verwenden wollen.

Eingabefeld	Beschreibung
DH-Gruppen	Wählen Sie aus der Liste der verfügbaren Diffie-Hellmann-Gruppen diejenigen aus, die Sie verwenden wollen.
SA-Lebensdauer	Geben Sie die gewünschte SA-Lebensdauer in Sekunden an.

Klicken Sie auf **Erstellen**.

Der Dialog **Sicherheits-Profil** schließt sich. Das neue Sicherheits-Profil wird zur Liste der verfügbaren Sicherheits-Profile in der Objektleiste hinzugefügt.

Virtuelle IP-Pools

Virtuelle IP-Pools können verwendet werden, um verbundenen Clients IP-Adressen-Konfigurationen zu schicken. Die virtuellen IP-Pools können in den Vorlagen und Verbindungen unter dem Tab **Tunnel** ausgewählt werden.

Unter **VPN** > **IPsec** > **Virtuelle IP-Pools** finden Sie zum einen die vordefinierten und nicht veränderbaren virtuellen IP-Pools für DHCP- und RADIUS-Server, zum anderen den **Default Virtual-IP pool**, den Sie bearbeiten können. Alternativ klicken Sie auf ⊕, um einen neuen virtuellen IP-Pool hinzuzufügen.

Die vordefinierten Profile können weder bearbeitet noch gelöscht werden.

Tabelle 8: Virtueller IP-Pool

Eingabefeld	Beschreibung
Name	Geben Sie diesem virtuellem IP-Pool einen aussagekräftigen Namen.
Verwendet in	Zeigt an, in welchen IPsec-Verbindungen dieser virtuelle IP-Pool aktuell verwendet wird.
IP-Pool	Netzwerk-Adresse, aus der IP-Adressen an die Clients geschickt werden.
Bevorzugter DNS-Server	IP-Adresse des bevorzugten DNS-Servers.
Alternativer DNS-Server	IP-Adresse des alternativen DNS-Servers.
Bevorzugter WINS-Server	IP-Adresse des bevorzugten WINS-Servers.
Alternativer WINS-Server	IP-Adresse des alternativen WINS-Servers.
DNS-Suchdomänen	Liste an DNS-Suchdomänen. Klicken Sie rechts auf ⊕, um Ihren Eintrag zur Liste der DNS-Suchdomänen hinzuzufügen.

Klicken Sie auf **Erstellen**.

Der Dialog **Virtueller IP-Pool** schließt sich. Der neue Pool wird zur Liste der verfügbaren virtuellen IP-Pools in der Objektleiste hinzugefügt.

Werden verwendete IP-Pools geändert, können in der erweiterten Listbar alle zugehörigen Verbindungen neu gestartet werden.

Vorlagen

Die Verbindungs-Vorlagen können verwendet werden, um Werte für Verbindungen vorzudefinieren, die häufig verwendet werden. Alle Werte außer dem Vorlagen-Namen sind optional und füllen das entsprechende Feld einer auf Basis dieser Vorlage erstellten VPN-Verbindung aus.

Es sind verschiedene Vorlagen vordefiniert, wie z. B. die Vorlage „LANCOM Advanced VPN Client“, um IPsec-Verbindungen mit diesem Client zu vereinfachen. Die Vorlage „(empty)“ kann verwendet werden, falls die Werte einer vorhandenen Verbindungen gelöscht werden sollen.

Die vordefinierten Vorlagen können weder bearbeitet noch gelöscht werden.

Unter **VPN** > **IPsec** > **Vorlagen** können Sie das Fenster **IPsec Verbindugs-Vorlage** öffnen. Im Fenster **IPsec Verbindungs-Vorlage** können Sie die folgenden Informationen einsehen und konfigurieren:

Tabelle 9: IPsec Verbindungs-Vorlage

Eingabefeld	Beschreibung
Name	Geben Sie dieser Vorlage einen aussagekräftigen Namen.
Sicherheits-Profil	Wählen Sie eines der vordefinierten Sicherheitsprofile aus.

Im Tab **Verbindung** können Sie Vorgaben für die folgenden Felder einstellen:

Tabelle 10: Verbindung

Eingabefeld	Beschreibung
Verbindung	Eine Netzwerk- oder Internet-Verbindung kann gewählt werden, deren IP-Adressen für die IPsec-Verbindung verwendet werden soll.
Listening-IP-Adressem	Alternativ zur **Verbindung** können auch benutzerdefinierte IP-Adressen eingetragen werden. Sind hier IP-Adressen gesetzt, so wird die Einstellung **Verbindung** ignoriert. Werden weder **Verbindung** noch **Listening-IP-Adressen** gesetzt, dann verwendet der IPsec-Dienst automatisch eine der konfigurierten IP-Adressen aller Verbindungen.
Remote Gateway	Diese Adresse ist für die Option **Verbindung aufbauen** notwendig, um die Adresse der Gegenstelle zu bestimmen.
Verbindung aufbauen	Von der Firewall wird eine Verbindung zur im Feld **Remote Gateway** angegebenen Adresse aufgebaut.
NAT-T erzwingen	Normalerweise wird NAT-T automatisch gesetzt, wenn die Verbindung es erfordert. Wenn dieser Automatismus nicht greift, dann kann über diese Option NAT-T für den Aufbau einer Verbindung erzwungen werden.

Im Tab **Tunnel** können Sie Vorgaben für die folgenden Felder einstellen:

Tabelle 11: Tunnel

Eingabefeld	Beschreibung
Lokale Netzwerke	Lokale Netzwerke, die mit der Gegenstelle verbunden werden sollen.
Remote Netzwerke	Remote-Netzwerke, die mit den lokalen Netzwerken verbunden werden sollen. Es werden alle konfigurierten lokalen mit allen konfigurierten entfernten (Remote) Netzwerken verbunden. Bei IKEv1-Verbindungen und IKEv2-Verbindungen mit aktivierter Option **IKEv2-Kompatibilitätsmodus** ist die maximale Anzahl an Kombinationen auf 25 begrenzt, bei IKEv2 mit inaktiver Option **IKEv2-Kompatibilitätsmodus** gibt es keine Begrenzung.
Virtueller IP-Pool	Der Gegenstelle wird eine IP-Adresse aus dem konfigurierten IP-Pool zugewiesen.
IKEv2-Kompatibilitätsmodus	Anstatt alle konfigurierten lokalen und entfernten Netze durch einen einzigen Tunnel zu schicken wird wie bei IKEv1 für jede Verbindung zwischen zwei Netzen ein einzelner Tunnel angelegt. Diese Option ist nur für IKEv2-Verbindungen gültig.

Im Tab **Authentifizierung** können Sie Vorgaben für die folgenden Felder einstellen:

Tabelle 12: Authentifizierung

Eingabefeld	Beschreibung
Authentifizierungstyp	Geben Sie den Authentifizierungstyp an. Mögliche Werte: › Zertifikat – die Authentifizierung wird über ein lokales und ein Remote-Zertifikat durchgeführt. › Certificate Authority – die Authentifizierung wird über ein lokales und ein Remote-Zertifikat durchgeführt, das von der ausgewählten CA signiert wurde. › PSK (Preshared Key) – die Authentizierung erfolgt über ein Passwort.
PSK (Preshared Key)	Nur bei Authentifizierungstyp PSK (Preshared Key) – Geben Sie das zu verwendende Passwort an.
Lokales Zertifikat	Das Zertifikat der Firewall zur Authentifizierung. Dieses muss einen Private Key beinhalten.
Lokaler Identifier	Ist diese Feld leer, wird bei PSK-Authentifizierung automatisch die ausgehende IP-Adresse der Firewall verwendet und bei Zertifikat-Authentifizierung der Distinguished Name (DN) des ausgewählten lokalen Zertifikats. › Bei PSK-Authentifizierung sind die folgenden Werte erlaubt: IP-Adressen, Fully Qualified Domain Names (FQDN), E-Mail Adressen (FQUN) und freier Text zwischen Anführungszeichen ("). › Bei Zertifikat-Authentifizierung sind die folgenden Werte erlaubt: Den Distinguished Name (DN) des ausgewählten Zertifikats, Wildcard DN – Alle DN Elemente müssen (in korrekter Reihenfolge) vorhanden sein, dürfen aber als Wildcard (z.B. CN=*) angegeben werden – eventuelle Subject Alternative Names (SAN) des ausgewählten Zertifikats.
Remote Zertifikat	Nur bei Authentifizierungstyp „Zertifikat": Zertifikat der Gegenstelle.
Certificate Authority	Nur bei Authentifizierungstyp „Certificate Authority": Eine CA, deren signierte Zertifikate für die Authentifizierung verwendet werden können.
Remote Identifier	Ist diese Feld leer, wird bei PSK-Authentifizierung automatisch die IP-Adresse des Remote Gateways verwendet, falls diese gesetzt wurde. Bei Zertifikat-Authentifizierung der Distinguished Name (DN) des ausgewählten remote Zertifikats. › Bei PSK-Authentifizierung sind die folgenden Werte erlaubt: IP-Adressen, Fully Qualified Domain Names (FQDN), E-Mail Adressen (FQUN) und freier Text zwischen Anführungszeichen ("). › Bei Zertifikat-Authentifizierung sind die folgenden Werte erlaubt: Den Distinguished Name (DN) des ausgewählten Zertifikats, Wildcard DN – Alle DN Elemente müssen (in korrekter Reihenfolge) vorhanden sein, dürfen aber als Wildcard (z.B. CN=*) angegeben werden – eventuelle Subject Alternative Names (SAN) des ausgewählten Zertifikats.
EAP / XAUTH	Aktiviert die Verwendung einer zusätzlichen Benutzer-Authentifizierung. Bei XAUTH für IKEv1 wird die lokale Benutzerdatenbank oder ein RADIUS Server verwendet (je nachdem ob in den IPsec-Einstellungen RADIUS aktiv ist oder nicht). Bei EAP für IKEv2 kann nur ein externer RADIUS Server verwendet werden, der in den IPsec-Einstellungen aktiviert sein muss. Die Konfiguration für den Radius-Server wird in den IPsec-Einstellungen vorgenommen.

Klicken Sie auf **Erstellen**.

Der Dialog **IPsec Verbindugs-Vorlage** schließt sich. Die neue Vorlage wird zur Liste der verfügbaren Vorlagen in der Objektleiste hinzugefügt.

IPsec-Verbindungen

Mit Ihrer LANCOM R&S®Unified Firewall können Sie Remote-Clients über IPsec (IPsec Client-to-Site) VPN-Zugang verschaffen und einen sicheren Tunnel zwischen zwei Remote-Netzwerken erstellen (IPsec Site-to-Site).

Übersicht IPSec-Verbindungen

Navigieren Sie zu **VPN** > **IPsec** > **Verbindungen**, um die Liste der derzeit im System angelegten IPSec-Verbindungen in der Objektleiste anzuzeigen.

In der erweiterten Ansicht wird in den Tabellenspalten der **Name** und der **Status** der IPSec-Verbindung angezeigt. Des Weiteren zeigen die Spalten die für diese Verbindung gewählte Authentifizierungsmethode an. Mit den Schaltflächen in der letzten Spalte können Sie die Einstellungen für eine IPsec-Verbindung einsehen und anpassen oder eine Verbindung aus dem System löschen.

Weitere Informationen finden Sie unter *Symbole und Schaltflächen*.

IPsec-Verbindungs-Einstellungen

Unter **VPN** > **IPsec** > **Verbindungen** können Sie eine IPsec-Verbindung hinzufügen, oder eine vorhandene Verbindung bearbeiten.

Im Bearbeitungsfenster **Verbindung** können Sie die folgenden Elemente konfigurieren:

Eingabefeld	Beschreibung
I/0	Ein Schiebeschalter gibt an, ob die IPSec-Verbindung derzeit aktiv (**I**) oder inaktiv (**0**) ist. Mit einem Klick auf den Schiebeschalter können Sie den Status der Verbindung ändern. Eine neue Verbindung ist standardmäßig aktiviert.
Name	Geben Sie einen eindeutigen Namen für die Verbindung ein. Dieser muss aus einem bis 63 alphanumerischen Zeichen und Unterstrichen bestehen.
Vorlage	Wählen Sie optional eine der vordefinierten Vorlagen aus. Alle Einstellungen werden entsprechend der gesetzten Werte aus der Vorlage verwendet. Werte die nicht in der Vorlage gesetzt wurden, werden zurückgesetzt. Daher kann die Vorlage „(empty)“ verwendet werden, um alle Werte zurückzusetzen.
Sicherheits-Profil	Wählen Sie eines der vordefinierten Sicherheitsprofile aus.

Im Tab **Verbindung** können Sie Vorgaben für die folgenden Felder einstellen:

Tabelle 13: Verbindung

Eingabefeld	Beschreibung
Verbindung	Eine Netzwerk- oder Internet-Verbindung kann gewählt werden, deren IP-Adressen für die IPsec-Verbindung verwendet werden soll.
Listening-IP-Adressem	Alternativ zur **Verbindung** können auch benutzerdefinierte IP-Adressen eingetragen werden. Klicken Sie rechts auf ⊕, um Ihren Eintrag zur Liste hinzuzufügen. Sind hier IP-Adressen gesetzt, so wird die Einstellung **Verbindung** ignoriert. Werden weder **Verbindung** noch **Listening-IP-Adressen** gesetzt, dann verwendet der IPsec-Dienst automatisch eine der konfigurierten IP-Adressen aller Verbindungen.
Remote Gateway	Diese Adresse ist für die Option **Verbindung aufbauen** notwendig, um die Adresse der Gegenstelle zu bestimmen.
Verbindung aufbauen	Von der Firewall wird eine Verbindung zur im Feld **Remote Gateway** angegebenen Adresse aufgebaut.
NAT-T erzwingen	Normalerweise wird NAT-T automatisch gesetzt, wenn die Verbindung es erfordert. Wenn dieser Automatismus nicht greift, dann kann über diese Option NAT-T für den Aufbau einer Verbindung erzwungen werden.

Im Tab **Tunnel** können Sie Vorgaben für die folgenden Felder einstellen:

Tabelle 14: Tunnel

Eingabefeld	Beschreibung
Lokale Netzwerke	Lokale Netzwerke, die mit der Gegenstelle verbunden werden sollen. Klicken Sie rechts auf ⊕, um Ihren Eintrag zur Liste hinzuzufügen.
Remote Netzwerke	Remote-Netzwerke, die mit den lokalen Netzwerken verbunden werden sollen. Klicken Sie rechts auf ⊕, um Ihren Eintrag zur Liste hinzuzufügen. Es werden alle konfigurierten lokalen mit allen konfigurierten entfernten (Remote) Netzwerken verbunden. Bei IKEv1-Verbindungen und IKEv2-Verbindungen mit aktivierter Option **IKEv2-Kompatibilitätsmodus** ist die maximale Anzahl an Kombinationen auf 25 begrenzt, bei IKEv2 mit inaktiver Option **IKEv2-Kompatibilitätsmodus** gibt es keine Begrenzung.
Virtueller IP-Pool	Der Gegenstelle wird eine IP-Adresse aus dem konfigurierten IP-Pool zugewiesen.
Virtuelle IP	Weisen Sie der Gegenstelle eine bestimmte IP-Adresse zu. Die Optionen **Remote-Netzwerke**, **Virtueller IP-Pool** und **Virtuelle IP** sollten nicht zusammen verwendet werden
IKEv2-Kompatibilitätsmodus	Anstatt alle konfigurierten lokalen und entfernten Netze durch einen einzigen Tunnel zu schicken wird wie bei IKEv1 für jede Verbindung zwischen zwei Netzen ein einzelner Tunnel angelegt. Diese Option ist nur für IKEv2-Verbindungen gültig.

Im Tab **Authentifizierung** können Sie Vorgaben für die folgenden Felder einstellen:

Tabelle 15: Authentifizierung

Eingabefeld	Beschreibung
Authentifizierungstyp	Geben Sie den Authentifizierungstyp an. Mögliche Werte: › Zertifikat – die Authentifizierung wird über ein lokales und ein Remote-Zertifikat durchgeführt. › Certificate Authority – die Authentifizierung wird über ein lokales und ein Remote-Zertifikat durchgeführt, das von der ausgewählten CA signiert wurde. › PSK (Preshared Key) – die Authentizierung erfolgt über ein Passwort.
PSK (Preshared Key)	Nur bei Authentifizierungstyp PSK (Preshared Key) – Geben Sie das zu verwendende Passwort an.
Lokales Zertifikat	Das Zertifikat der Firewall zur Authentifizierung. Dieses muss einen Private Key beinhalten.
Lokaler Identifier	Ist diese Feld leer, wird bei PSK-Authentifizierung automatisch die ausgehende IP-Adresse der Firewall verwendet und bei Zertifikat-Authentifizierung der Distinguished Name (DN) des ausgewählten lokalen Zertifikats. › Bei PSK-Authentifizierung sind die folgenden Werte erlaubt: IP-Adressen, Fully Qualified Domain Names (FQDN), E-Mail Adressen (FQUN) und freier Text zwischen Anführungszeichen ("). › Bei Zertifikat-Authentifizierung sind die folgenden Werte erlaubt: Den Distinguished Name (DN) des ausgewählten Zertifikats, Wildcard DN – Alle DN Elemente müssen (in korrekter Reihenfolge) vorhanden sein, dürfen aber als Wildcard (z.B. CN=*) angegeben werden – eventuelle Subject Alternative Names (SAN) des ausgewählten Zertifikats.
Remote Zertifikat	Nur bei Authentifizierungstyp „Zertifikat": Zertifikat der Gegenstelle.
Certificate Authority	Nur bei Authentifizierungstyp „Certificate Authority": Eine CA, deren signierte Zertifikate für die Authentifizierung verwendet werden können.

Eingabefeld	Beschreibung
Remote Identifier	Ist diese Feld leer, wird bei PSK-Authentifizierung automatisch die IP-Adresse des Remote Gateways verwendet, falls diese gesetzt wurde. Bei Zertifikat-Authentifizierung der Distinguished Name (DN) des ausgewählten remote Zertifikats. › Bei PSK-Authentifizierung sind die folgenden Werte erlaubt: IP-Adressen, Fully Qualified Domain Names (FQDN), E-Mail Adressen (FQUN) und freier Text zwischen Anführungszeichen ("). › Bei Zertifikat-Authentifizierung sind die folgenden Werte erlaubt: Den Distinguished Name (DN) des ausgewählten Zertifikats, Wildcard DN – Alle DN Elemente müssen (in korrekter Reihenfolge) vorhanden sein, dürfen aber als Wildcard (z.B. CN=*) angegeben werden – eventuelle Subject Alternative Names (SAN) des ausgewählten Zertifikats.
EAP / XAUTH	Aktiviert die Verwendung einer zusätzlichen Benutzer-Authentifizierung. Bei XAUTH für IKEv1 wird die lokale Benutzerdatenbank oder ein RADIUS Server verwendet (je nachdem ob in den IPsec-Einstellungen RADIUS aktiv ist oder nicht). Bei EAP für IKEv2 kann nur ein externer RADIUS Server verwendet werden, der in denIPsec-Einstellungen aktiviert sein muss. Die Konfiguration für den Radius-Server wird in den IPsec-Einstellungen vorgenommen

Die Schaltflächen rechts unten im Bearbeitungsfeld hängen davon ab, ob Sie eine neue VPN-IPsec-Verbindung hinzufügen oder eine bestehende Verbindung bearbeiten. Klicken Sie für eine neu konfigurierte Netzwerkverbindung auf **Erstellen**, um die Verbindung zur Liste der verfügbaren IPSec-Netzwerkverbindungen hinzuzufügen, oder auf **Abbrechen**, um die Erstellung einer neuen Netzwerkverbindung abzubrechen.

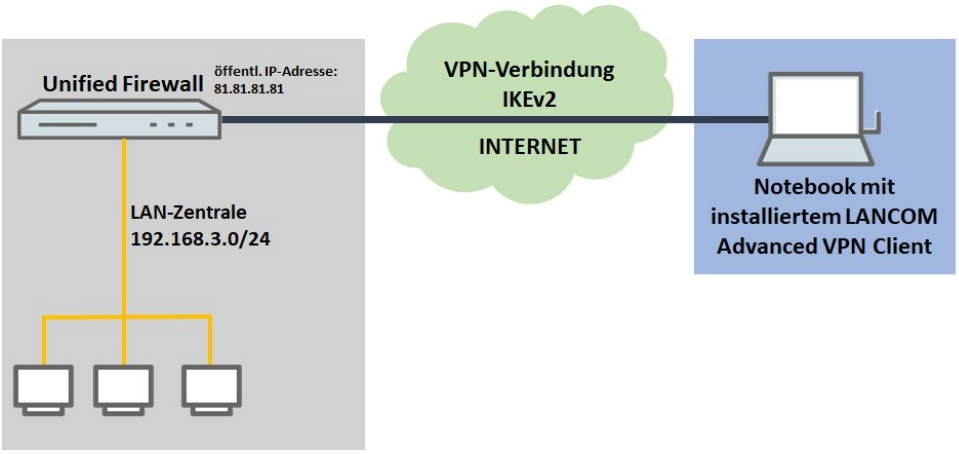
Wenn Sie Änderungen vorgenommen haben, können Sie diese mit den Schaltflächen unten rechts im Bearbeitungsfenster speichern (**Speichern**) oder verwerfen (**Zurücksetzen**). Andernfalls können Sie das Fenster schließen (**Schließen**).

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

Einrichtung einer IKEv2 VPN-Verbindung mit dem LANCOM Advanced VPN-Client

Szenario: Die LANCOM R&S®Unified Firewall ist direkt mit dem Internet verbunden und verfügt über eine öffentliche IPv4-Adresse:

› Ein Unternehmen möchte seinen Außendienst-Mitarbeitern den Zugriff auf das Firmennetzwerk per IKEv2 Client-To-Site Verbindung ermöglichen.
› Dazu ist auf den Notebooks der Außendienst-Mitarbeiter der LANCOM Advanced VPN Client installiert.
› Die Firmenzentrale verfügt über eine LANCOM R&S®Unified Firewall als Gateway und eine Internetverbindung mit der festen öffentlichen IP-Adresse 81.81.81.81.
› Das lokale Netzwerk der Zentrale hat den IP-Adressbereich 192.168.3.0/24.

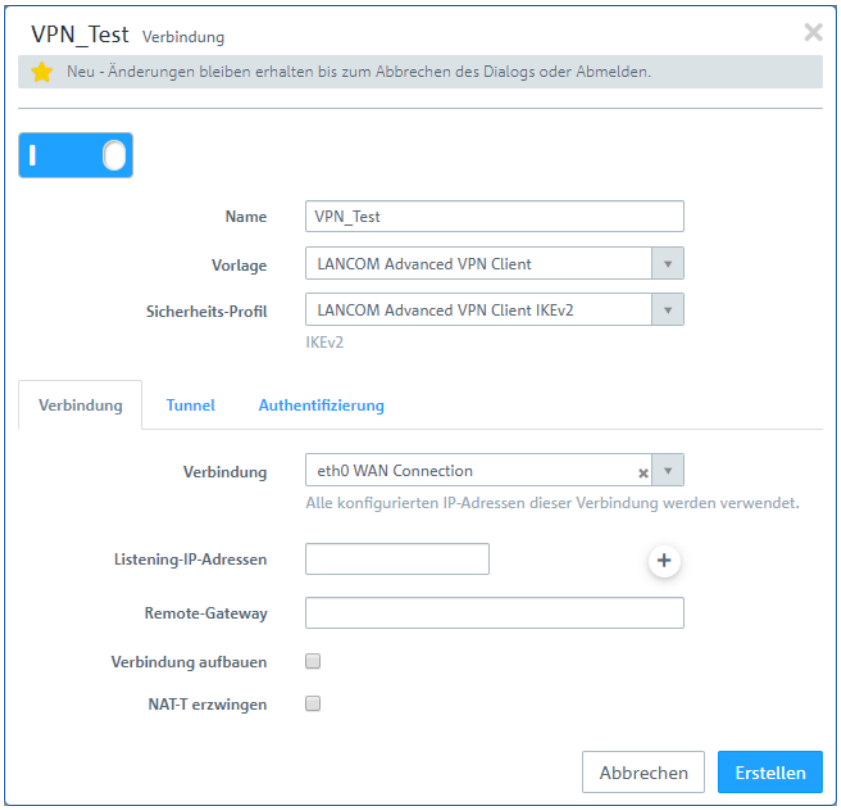


Konfigurationsschritte auf der LANCOM R&S®Unified Firewall

1. Verbinden Sie sich mit der Konfigurationsoberfläche der Unified Firewall und wechseln auf **VPN** > **IPsec** > **IPsec-Einstellungen**
2. Aktivieren Sie IPsec, indem Sie es über den Schiebeschalter oben links einschalten. Speichern Sie diese Änderung.
3. Wechseln Sie auf **VPN** > **IPsec** > **Verbindungen** und klicken auf ⊕, um eine neue IPsec-Verbindung zu erstellen.
4. Speichern Sie die folgenden Parameter:
   - Name: Vergeben Sie einen aussagekräftigen Namen.

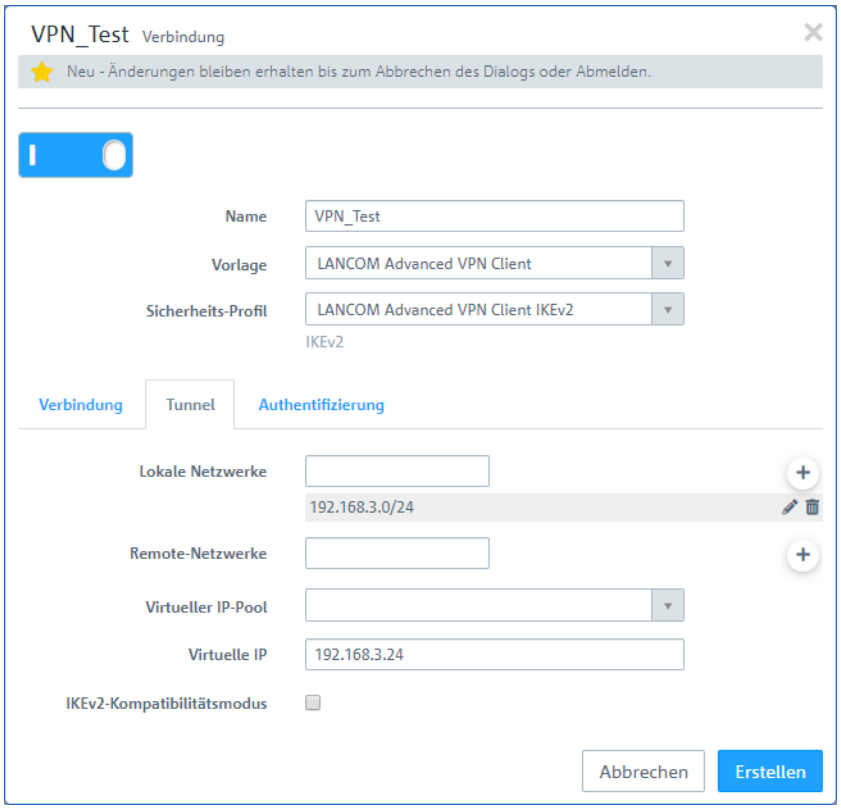
     Der Name darf nur Buchstaben, Zahlen und Unterstriche enthalten!

   - Vorlage: Wählen Sie „LANCOM Advanced VPN Client".
   - Netzwerk-Verbindung: Wählen Sie im Dropdown-Menü das WAN-Objekt aus, welches für die Internet-Verbindung verwendet wird.



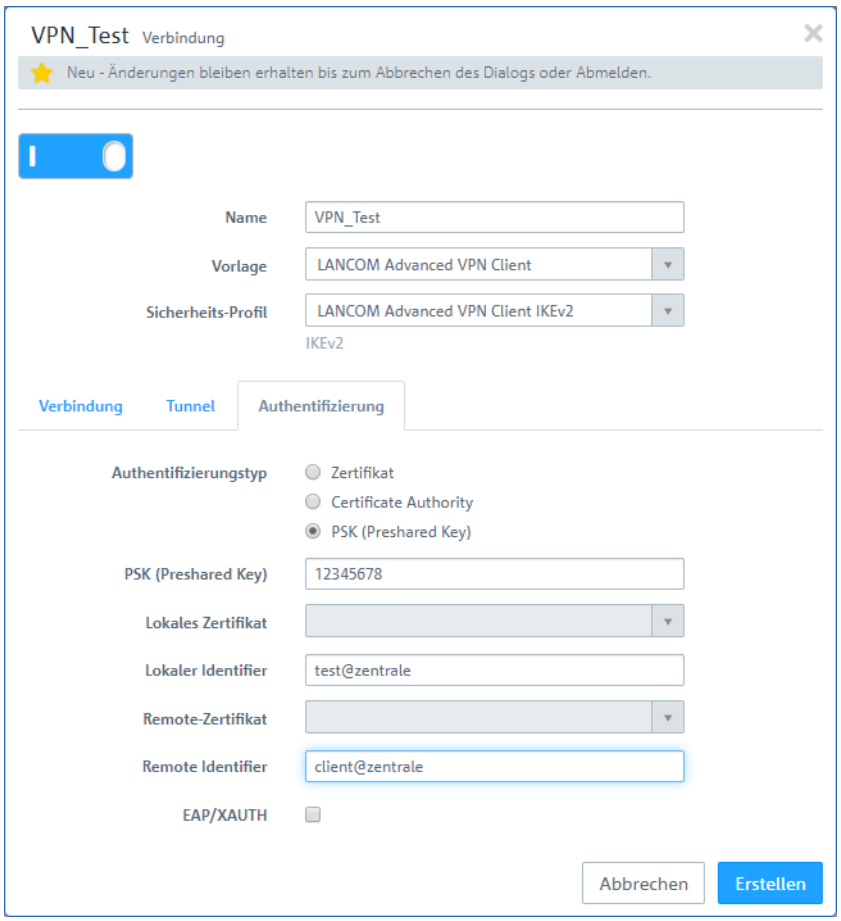
5. Wechseln Sie zum Reiter Tunnel und hinterlegen folgende Parameter:
   - Lokale Netzwerke: Hinterlegen Sie das lokale Netzwerk in CIDR-Schreibweise (Classless Inter-Domain Routing), mit dem der VPN-Client kommunizieren soll.
   - Virtueller IP-Pool: Entfernen Sie mit einem Klick auf das rechte x den voreingestellten virtuellen IP-Pool.

- Virtuelle IP: Weisen Sie dem VPN-Client eine IP-Adresse aus dem lokalen Netzwerk zu. Diese IP-Adresse wird dem VPN-Client bei jeder Einwahl über den IKE-Config-Mode zugeteilt.

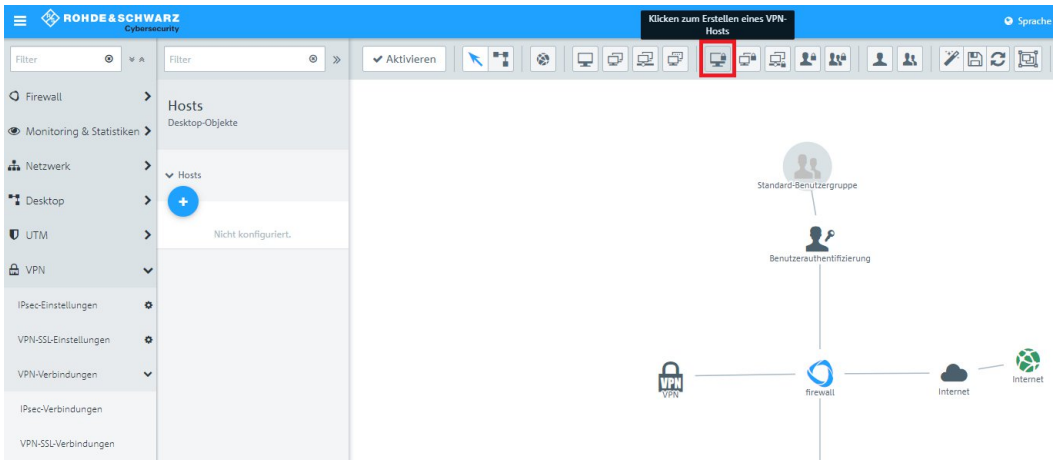


6. Wechseln Sie zum Reiter Authentifizierung und hinterlegen folgende Parameter:
   - Authentifizierungstyp: Wählen Sie „PSK (Preshared Key)“ aus.
   - PSK (Preshared Key): Vergeben Sie einen Preshared Key.
   - Lokaler Identifier: Bestimmen Sie die lokale Identität.
   - Remote Identifier: Bestimmen Sie die entfernte Identität.

Der Local und Remote Identifier dürfen nicht übereinstimmen!

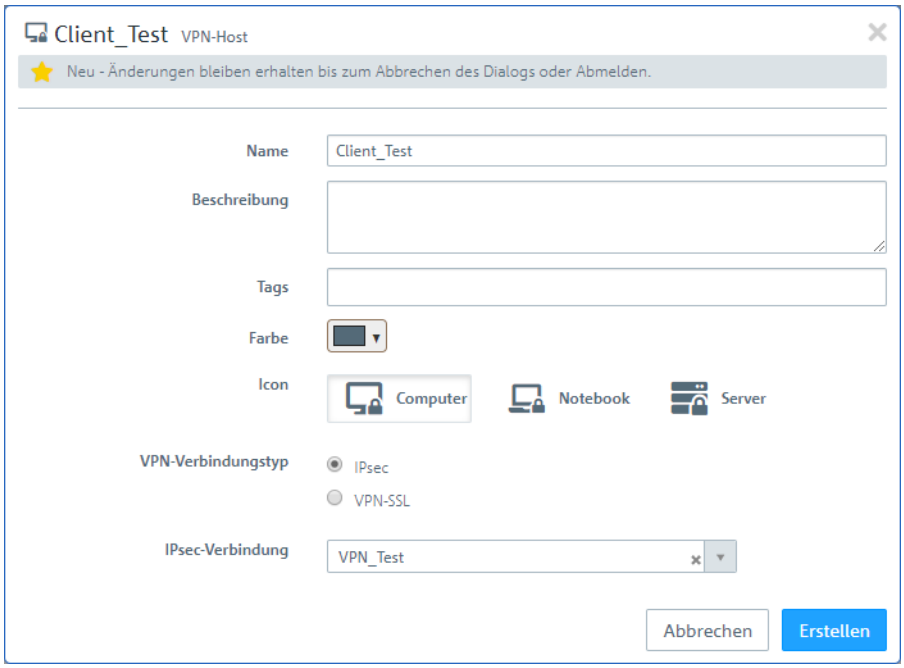


7. Klicken Sie auf Erstellen, um die Verbindung anzulegen.
8. Um einen neuen VPN-Host anzulegen, klicken Sie auf .



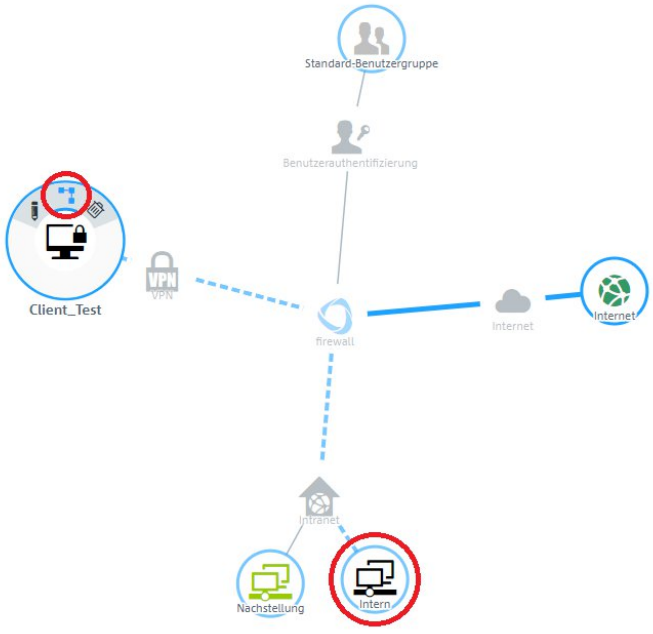
9. Speichern Sie die folgenden Parameter:
   - Name: Vergeben Sie einen aussagekräftigen Namen.
   - VPN-Verbindungstyp: Wählen Sie den Typ IPsec.

› IPSec-Verbindung: Wählen Sie im Dropdownmenü bei IPsec die in Schritt *3* auf Seite 28 bis *7* auf Seite 30 erstellte VPN-Verbindung aus.



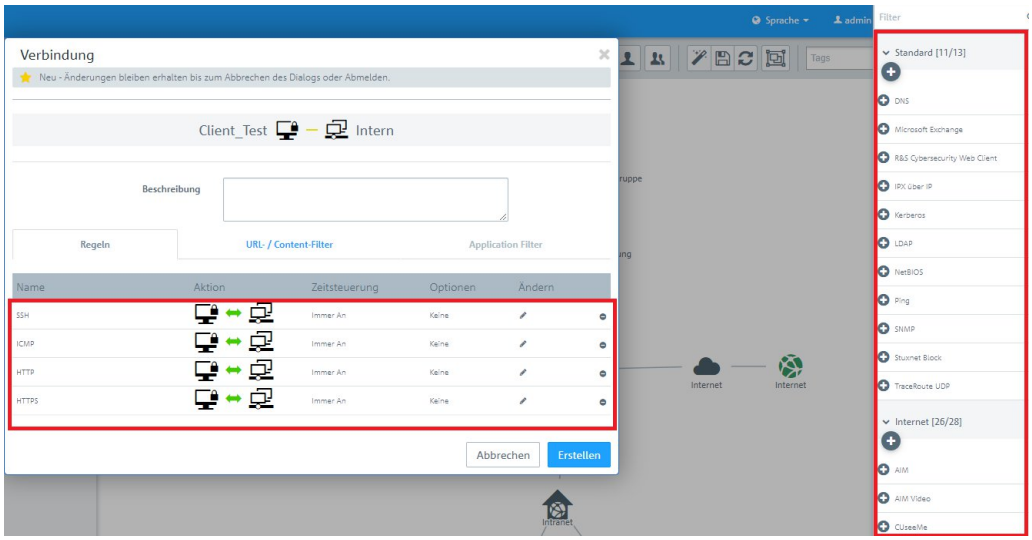
10. Klicken Sie im VPN-Host auf und klicken anschließend auf das Netzwerk-Objekt, auf welches der LANCOM Advanced VPN Client zugreifen können soll, damit die Firewall-Objekte geöffnet werden.

Wiederholen Sie diesen Schritt für jedes weitere interne Netzwerk, auf das der LANCOM Advanced VPN Client Zugriff haben soll.

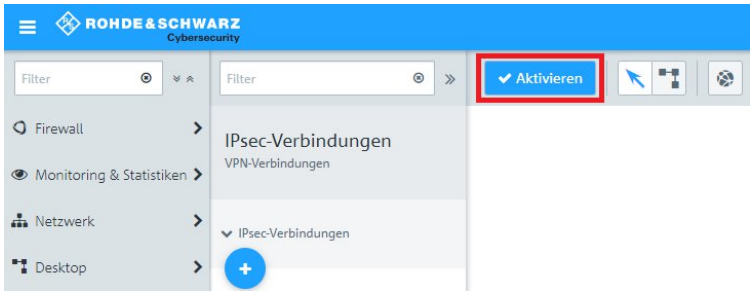


11. Weisen Sie über ⊕ die erforderlichen Protokolle dem VPN-Host zu.

Eine LANCOM R&S®Unified Firewall verwendet eine Deny-All Strategie. Die Kommunikation muss also explizit erlaubt werden.



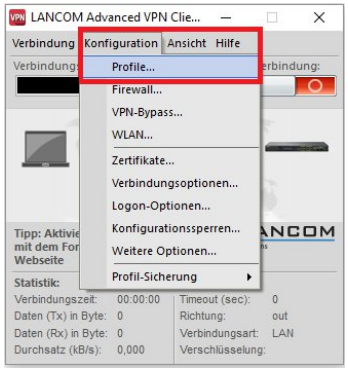
12. Klicken Sie zuletzt auf ✔ **Aktivieren**, damit die Konfigurations-Änderungen umgesetzt werden.



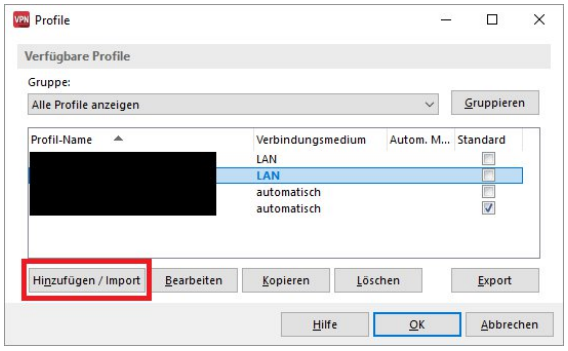
13. Die Konfigurationsschritte auf der Unified Firewall sind damit abgeschlossen.

Konfigurationsschritte im LANCOM Advanced VPN Client:

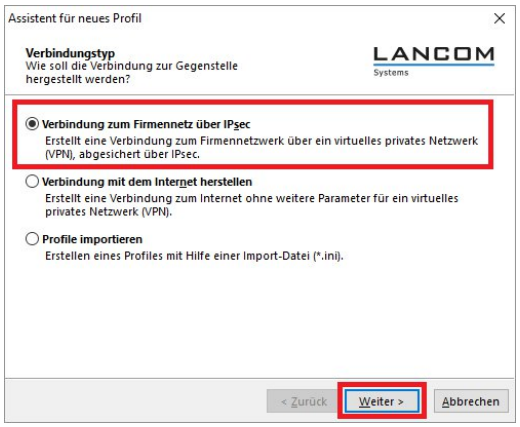
1. Öffnen Sie den LANCOM Advanced VPN Client und wechseln in das Menü **Configuration** > **Profiles**.



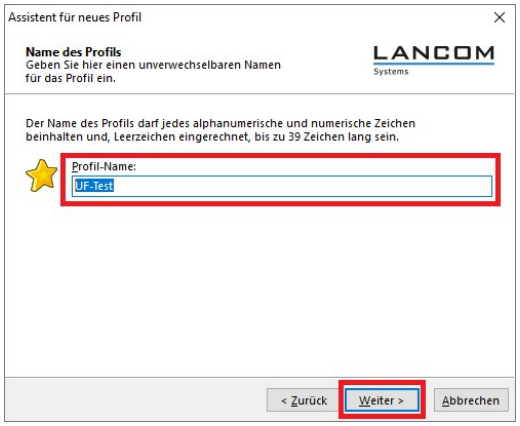
2. Klicken Sie auf **Add / Import**, um einen neuen VPN-Zugang zu erstellen.



3. Wählen Sie **Link to Corporate Network Using IPSec**.

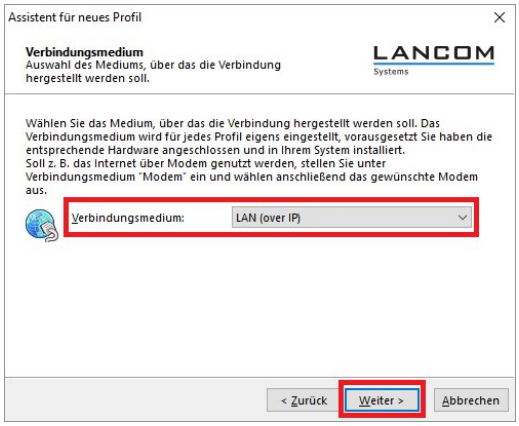


4. Vergeben Sie einen aussagekräftigen Namen.

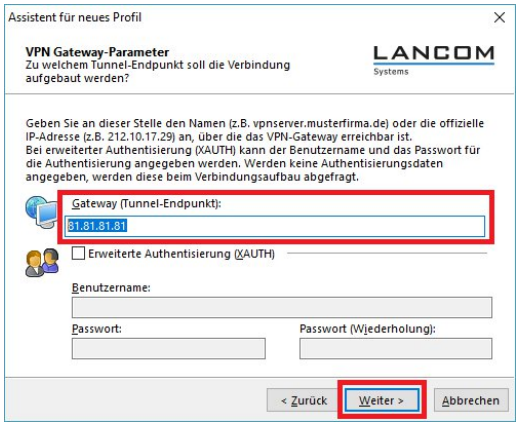


5. Wählen Sie das Verbindungsmedium aus.

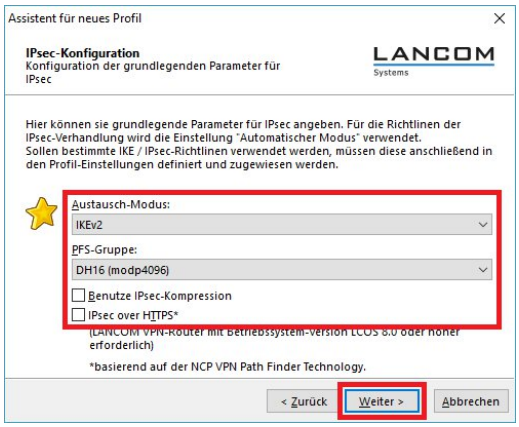
Werden wechselnde Verbindungsmediem verwendet (z. B. LAN und WLAN), verwenden Sie die Option automatische Medienerkennung.



6. Geben Sie die öffentliche IP-Adresse oder den DynDNS-Namen der Unified Firewall an.



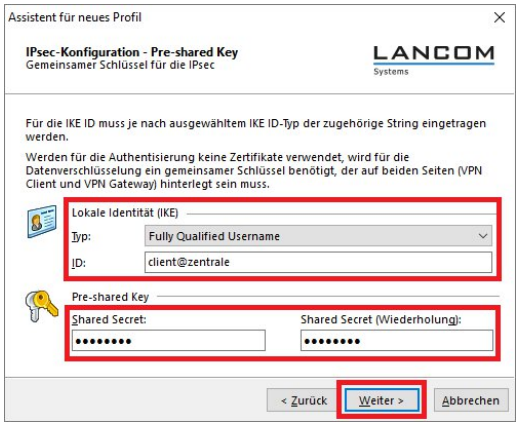
7. Setzen Sie den **Exchange Mode** auf „IKEv2“ und die **PFS-Group** auf „DH16 (modp4096)“. Deaktivieren Sie die Funktion **IPsec-over-HTTPS**.



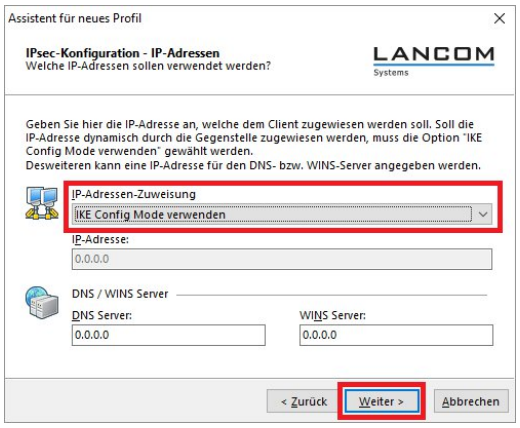
8. Speichern Sie die folgenden Parameter:

   - **Typ**: Wählen Sie im Dropdown-Menü den Identitätstyp Fully Qualified Username (FQUN) aus.
   - **ID**: Hinterlegen Sie den Remote Identifier, vergeben im Schritt *6* auf Seite 29

› **Shared Secret**: Hinterlegen Sie den im Schritt *6* auf Seite 29 vergebenen Preshared Key.

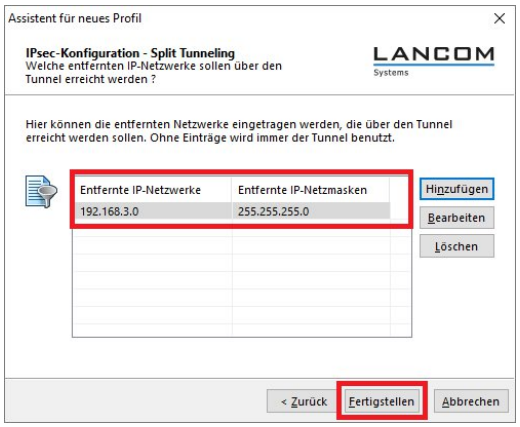


9. Wählen Sie im Dropdown-Menü „IKE Config Mode“ aus, damit dem VPN-Client die IP-Adresse automatisch durch die LANCOM R&S®Unified Firewall zugewiesen wird.



10. Hinterlegen Sie zur Verwendung der Funktion Split Tunneling das Zielnetz, welches über den VPN-Tunnel erreicht werden soll.

Ohne konfiguriertes Split-Tunneling wird bei aufgebautem VPN-Tunnel aller Datenverkehr über den VPN-Tunnel übertragen, also auch der für das lokale Netzwerk oder das Internet bestimmte Datenverkehr. Dies kann zu Kommunikations-Problemen führen!

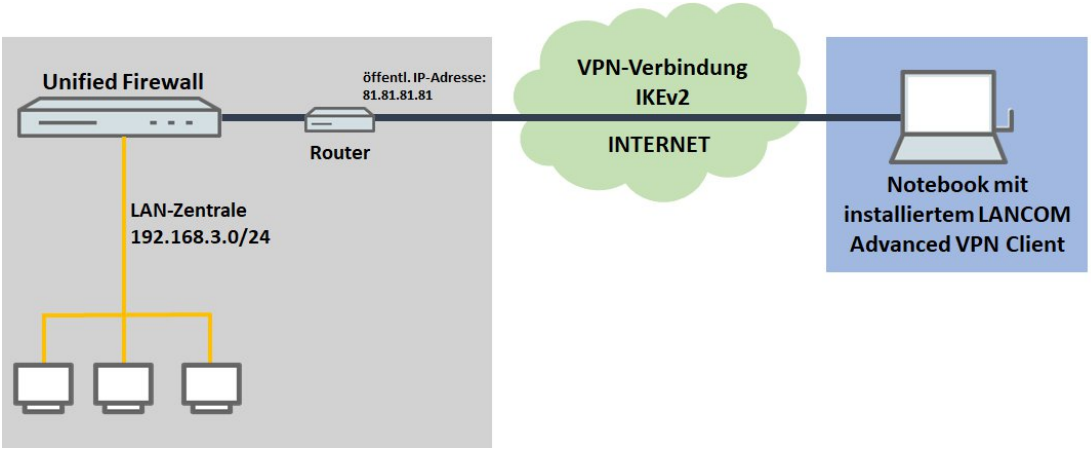


11. Die Konfigurationsschritte im LANCOM Advanced VPN Client sind damit abgeschlossen.

Zusätzliche Schritte für eine „Parallel" Lösung

Szenario: Die LANCOM R&S®Unified Firewall geht über einen vorgeschalteten Router ins Internet:

- Ein Unternehmen möchte seinen Außendienst-Mitarbeitern den Zugriff auf das Firmennetzwerk per IKEv2 Client-To-Site Verbindung ermöglichen.
- Dazu ist auf den Notebooks der Außendienst-Mitarbeiter der LANCOM Advanced VPN Client installiert.
- Die Firmenzentrale verfügt über eine LANCOM R&S®Unified Firewall als Gateway und einen vorgeschalteten Router, welcher die Internet-Verbindung herstellt. Der Router hat die feste öffentliche IP-Adresse 81.81.81.81.
- Das lokale Netzwerk der Zentrale hat den IP-Adressbereich 192.168.3.0/24.

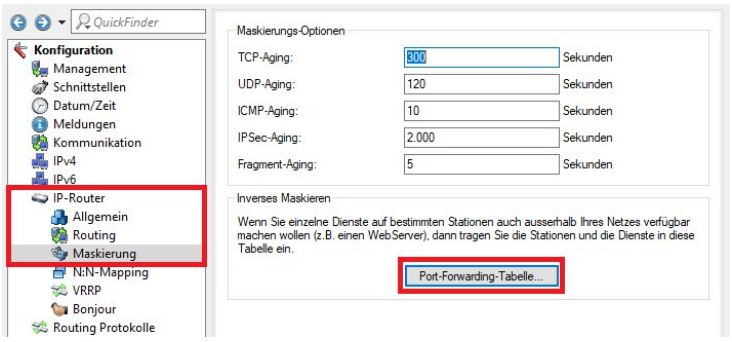


Bei diesem Szenario muss zusätzlich ein Port- und Protokollforwarding auf dem vorgeschalteten Router eingerichtet werden.

Für IPSec werden die UDP-Ports 500 und 4500 sowie das Protokoll ESP benötigt. Diese müssen auf die Unified Firewall weitergeleitet werden. Werden die UDP-Ports 500 und 4500 weitergeleitet, wird das Protokoll ESP automatisch mit weitergeleitet.

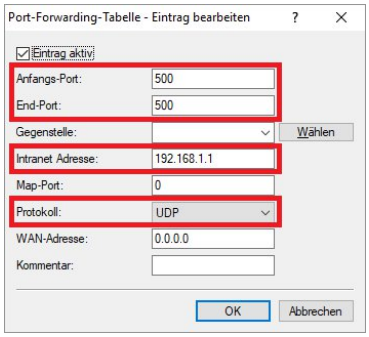
Werden die UDP-Ports 500 und 4500 sowie das Protokoll ESP auf die LANCOM R&S®Unified Firewall weitergeleitet, kann eine IPSec-Verbindung auf dem LANCOM Router nur noch verwendet werden, wenn diese in HTTPS gekapselt wird (IPSec-over-HTTPS). Ansonsten kann keine IPSec-Verbindung mehr aufgebaut werden.

1. Öffnen Sie die Konfiguration des Routers in LANconfig und wechseln in das Menü **IP-Router** > **Maskierung.** > **Port-Forwarding-Tabelle**.

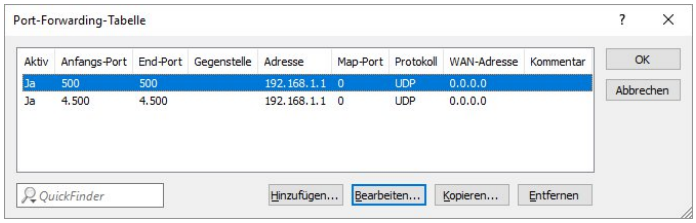


2. Speichern Sie die folgenden Parameter:
   - **Anfangs-Port**: Hinterlegen Sie den Port 500.
   - **End-Port**: Hinterlegen Sie den Port 500.
   - **Intranet-Adresse**: Hinterlegen Sie die IP-Adresse der LANCOM R&S®Unified Firewall im Transfernetz zwischen LANCOM R&S®Unified Firewall und dem LANCOM Router.

> **Protokoll**: Wählen Sie im Dropdown-Menü UDP aus.



3. Erstellen Sie einen weiteren Eintrag und hinterlegen den UDP-Port 4500.



4. Schreiben Sie die Konfiguration in den Router zurück.

8.1.2 VPN-SSL

VPN über SSL bietet eine schnelle und sichere Möglichkeit, eine Roadwarrior-Verbindung einzurichten. Der größte Vorteil von VPN-SSL ist, dass der gesamte Datenverkehr über einen TCP- oder UDP-Port läuft und keine weiteren speziellen Protokolle benötigt werden.

Ihre LANCOM R&S®Unified Firewall ermöglicht es Ihnen, Remote-Clientcomputern einen VPN-Zugang zu gewähren (C2S, „Client-to-Site“), oder eine sichere Verbindung zwischen zwei Remote-Netzwerken (S2S, „Site-to-Site“) über das VPN-SSL-Protokoll herzustellen.

VPN-SSL-Einstellungen

Unter **VPN** > **VPN-SSL** > **VPN-SSL-Einstellungen** können Sie VPN-SSL aktivieren und die allgemeinen Einstellungen dazu auf Ihrer LANCOM R&S®Unified Firewall konfigurieren:

Eingabefeld	Beschreibung
I/0	Ein Schiebeschalter gibt an, ob VPN-SSL aktiv (**I**) oder inaktiv (**0**) ist. Mit einem Klick auf den Schiebeschalter ändern Sie den Status dieser Option.
Host-Zertifikat	Wählen Sie ein Hostzertifikat aus, das Ihre LANCOM R&S®Unified Firewall für alle VPN-SSL-Verbindungen nutzt.
DNS	Optional: Geben Sie einen DNS-Server ein, der von Clients für Client-to-Site-Verbindungen verwendet werden soll, während die Verbindung besteht.
WINS	Optional: Geben Sie einen WINS-Server ein, der von Clients für Client-to-Site-Verbindungen verwendet werden soll, während die Verbindung besteht.
Timeout	Geben Sie die Zeitüberschreitung in Sekunden ein. Der Tunnel wird getrennt, wenn bis zur Zeitüberschreitung kein Datenfluss vorliegt. Die Standardeinstellung beträgt `0`. Der Tunnel wird also permanent aufrechterhalten.
Log-Level	Legen Sie die Ereignisprotokollstufe fest. Für Troubleshooting empfiehlt sich die Ereignisprotokollstufe `5` .

Eingabefeld	Beschreibung
Routen	Geben Sie Routen für die VPN-SSL-Tunnel ein, die von den Clients oder dem entfernten Verbindungsende erstellt werden sollen. Diese Routen werden dann für alle VPN-SSL-Verbindungen verwendet. Klicken Sie auf **Hinzufügen**, um die Route zur Liste hinzuzufügen. Sie können einzelne Einträge in der Liste bearbeiten oder löschen, indem Sie auf die entsprechende Schaltfläche neben einem Eintrag klicken. Weitere Informationen finden Sie unter *Symbole und Schaltflächen*. Wenn Sie einen Eintrag bearbeiten, erscheint auf der rechten Seite des Eintrags ein Haken. Klicken Sie auf den Haken, um Ihre Änderungen zu übernehmen.

Im Tab **Client-to-Site** :

Eingabefeld	Beschreibung
Protokoll	Wählen Sie das zu verwendende Protokoll aus, indem Sie die entsprechende Optionsschaltfläche auswählen.
Port	Geben Sie die Nummer des VPN-SSL Listening Port an, der für eingehende Verbindungen verwendet werden soll. Die gleiche Port-Nummer muss auch in der Client-Software angegeben werden.
Adressbereich	Geben Sie den Adressbereich an, aus dem IP-Adressen an Clients vergeben werden. Der Adressbereich darf sich nicht mit Ihren lokalen Netzwerken überschneiden.
Verschlüsselungs-Algorithmus	Wählen Sie aus der Drop-down-Liste den Verschlüsselungsalgorithmus aus, der für C2S-Verbindungen über VPN-SSL verwendet werden soll.
Erneute Verhandlung des Schlüssels	Um die Sicherheit zu erhöhen, erneuert eine VPN-SSL-Verbindung den Sitzungsschlüssel, während die Verbindung besteht. Geben Sie das Intervall für diese Schlüsselerneuerung in Sekunden an.
Kompression	Optional: Entfernen Sie dieses Häkchen, um LZO (Lempel-Ziv-Oberhumer, ein Algorithmus für verlustfreie Datenkompression) zu deaktivieren. Dieses Kontrollkästchen ist standardmäßig aktiviert.

Im Tab **Site-to-Site** :

Eingabefeld	Beschreibung
Protokoll	Wählen Sie das zu verwendende Protokoll aus, indem Sie die entsprechende Optionsschaltfläche auswählen.
Port	Geben Sie die Nummer des VPN-SSL Listening Port an, der für eingehende Verbindungen verwendet werden soll. Dieselbe Portnummer muss am entfernten Verbindungsende angegeben werden.
Adressbereich	Geben Sie den Adressbereich an, aus dem IP-Adressen für S2S-Verbindungen verwendet werden sollen. Der Adressbereich darf sich nicht mit Ihren lokalen Netzwerken überschneiden.
Verschlüsselungs-Algorithmus	Wählen Sie aus der Drop-down-Liste den Verschlüsselungsalgorithmus aus, der für S2S-Verbindungen über VPN-SSL verwendet werden soll.
Erneute Verhandlung des Schlüssels	Um die Sicherheit zu erhöhen, erneuert eine VPN-SSL-Verbindung den Sitzungsschlüssel, während die Verbindung besteht. Geben Sie das Intervall für diese Schlüsselerneuerung in Sekunden an.

Eingabefeld	Beschreibung
Kompression	Optional: Entfernen Sie dieses Häkchen, um LZO (Lempel-Ziv-Oberhumer, ein Algorithmus für verlustfreie Datenkompression) zu deaktivieren. Dieses Kontrollkästchen ist standardmäßig aktiviert.

Wenn Sie Änderungen vorgenommen haben, können Sie diese mit den Schaltflächen unten rechts im Bearbeitungsfenster speichern (**Speichern**) oder verwerfen (**Zurücksetzen**). Andernfalls können Sie das Fenster schließen (**Schließen**).

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

VPN-SSL-Verbindungen

Unter **VPN** > **VPN-SSL** > **VPN-SSL-Verbindungen** können Sie VPN-SSL-Verbindungen erstellen und verwalten.

Mit Ihrer LANCOM R&S®Unified Firewall können Sie Remote-Clients über VPN-SSL (Client-to-Site) VPN-Zugang verschaffen und einen sicheren Tunnel zwischen zwei Remote-Netzwerken erstellen (Site-to-Site).

Übersicht VPN-SSL-Verbindungen

Navigieren Sie zu **VPN** > **VPN-SSL** > **VPN-SSL-Verbindungen**, um die Liste der derzeit im System angelegten VPN-SSL-Verbindungen in der Objektleiste anzuzeigen.

In der erweiterten Ansicht wird in den Tabellenspalten der **Name** der VPN-SSL-Verbindung, das für die Verbindung verwendete **Zertifikat** sowie der **Typ** und der **Status** der Verbindung angezeigt. Mit den Schaltflächen in der letzten Spalte können Sie die Einstellungen für eine VPN-SSL-Verbindung einsehen und anpassen oder eine Verbindung aus dem System löschen.

Weitere Informationen finden Sie unter *Symbole und Schaltflächen*.

VPN-SSL-Verbindungseinstellungen

Unter **VPN** > **VPN-SSL** > **VPN-SSL-Verbindungen** können Sie eine VPN-SSL-Verbindung hinzufügen, oder eine vorhandene Verbindung bearbeiten.

Mit den Einstellungen unter **VPN-SSL-Verbindungen** können Sie die folgenden Elemente konfigurieren:

Eingabefeld	Beschreibung
I/0	Ein Schiebeschalter gibt an, ob die VPN-SSL-Verbindung derzeit aktiv (**I**) oder inaktiv (**0**) ist. Mit einem Klick auf den Schiebeschalter können Sie den Status der Verbindung ändern. Neu angelegte Verbindungen sind standardmäßig aktiviert.
Name	Geben Sie einen eindeutigen Namen für die Verbindung ein. Der Name muss aus alphanumerischen Zeichen bestehen (erlaubt sind Buchstaben mit Ausnahme von ä, ö, ü und ß sowie Zahlen und Sonderzeichen).
Zertifikat	Wählen Sie das Serverzertifikat für VPN-SSL-Verbindungen aus der Drop-Down-Liste aus. Das VPN-Zertifikat muss an allen Standorten von der gleichen Zertifizierungsstelle (Certificate Authority, CA) signiert werden. Es empfiehlt sich daher, die VPN-Zertifizierungsstelle und die VPN-Zertifikate an einem Standort zu verwalten und die VPN-Zertifikate von dort an alle weiteren Standorte zu exportieren.
Verbindungstyp	Wählen Sie den Typ der Verbindung und die Funktion der LANCOM R&S®Unified Firewall aus, indem Sie die entsprechende Optionsschaltfläche auswählen. Sie können aus den folgenden drei Typen auswählen: › **Client-to-Site** – Es wird eine C2S-Verbindung hergestellt (z. B. für Full Tunneling). Dieser Verbindungstyp kann z. B. mit dem herkömmlichen OpenVPN-Client verwendet werden, um vor allem mobile Clients mit Ihrem lokalen Netzwerk zu verbinden.

Eingabefeld	Beschreibung
	› **Site-to-Site (Server)** – Es wird eine S2S-Verbindung hergestellt, bei der Ihre LANCOM R&S®Unified Firewall als Server dient. › **Site-to-Site (Client)** – Es wird eine S2S-Verbindung hergestellt. Ihre LANCOM R&S®Unified Firewall dient als Client.

Die angezeigten Elemente in den Einstellungen hängen vom gewählten Verbindungstyp ab:

Bei Client-to-Site-Verbindungen können Sie die folgende Elemente konfigurieren:

Eingabefeld	Beschreibung
Standard Gateway setzen	Setzen Sie den Haken in diesem Kontrollkästchen, um den VPN-SSL-Tunnel als Standard-Route zu verwenden (z. B. für Full Tunneling).
Client IP	Optional: Geben Sie die IP-Adresse ein, unter der der Client erreichbar ist.
Zusätzliche Server-Netzwerke	Die Angabe der lokalen Netzwerke, zu denen der Client Verbindungsrouten erstellen soll, muss in gültiger CIDR-Notation erfolgen (IP-Adresse gefolgt von einem Schrägstrich „/" und der Anzahl der in der Subnetzmaske festgelegten Bits, z. B. `192.168.1.0/24`). Klicken Sie auf **Hinzufügen**, um ein Netzwerk zur Liste hinzuzufügen. Sie können einzelne Einträge in der Liste bearbeiten oder löschen, indem Sie auf die entsprechende Schaltfläche neben einem Eintrag klicken. Weitere Informationen finden Sie unter *Symbole und Schaltflächen*. Wenn Sie einen Eintrag bearbeiten, erscheint auf der rechten Seite des Eintrags ein Haken. Klicken Sie auf den Haken, um Ihre Änderungen zu übernehmen.

Bei Site-to-Site-Verbindungenn, bei denen Ihre LANCOM R&S®Unified Firewall als Server dient, können Sie die folgenden Elemente konfigurieren:

Eingabefeld	Beschreibung
Adressbereich	Geben Sie den Adressbereich an, aus dem IP-Adressen für diese Verbindung verwendet werden. Der Adressbereich ist in den Einstellungen für VPN-SSL angegeben. Weitere Informationen finden Sie unter *VPN-SSL* auf Seite 37.
Remote-IP	Optional: Geben Sie die IP-Adresse des entfernten Verbindungsendes ein.
Fremde Netzwerke	Geben Sie die Netzwerke an, die dem entfernten Verbindungsende zur Verfügung stehen. Nachdem die Verbindung erfolgreich hergestellt wurde, erstellt der Server Routen in diesen Netzwerken. Klicken Sie auf **Hinzufügen**, um ein Netzwerk zur Liste hinzuzufügen. Sie können einzelne Einträge in der Liste bearbeiten oder löschen, indem Sie auf die entsprechende Schaltfläche neben einem Eintrag klicken. Weitere Informationen finden Sie unter *Symbole und Schaltflächen*. Wenn Sie einen Eintrag bearbeiten, erscheint auf der rechten Seite des Eintrags ein Haken. Klicken Sie auf den Haken, um Ihre Änderungen zu übernehmen.
Zusätzliche eigene Netzwerke	Geben Sie zusätzliche lokale Netzwerke an. Nachdem die Verbindung erfolgreich hergestellt wurde, erstellt der Server Routen in diesen Netzwerken. Klicken Sie auf **Hinzufügen**, um ein Netzwerk zur Liste hinzuzufügen. Sie können einzelne Einträge in der Liste bearbeiten oder löschen, indem Sie auf die entsprechende Schaltfläche neben einem Eintrag klicken. Weitere Informationen finden Sie unter *Symbole und Schaltflächen*.

Eingabefeld	Beschreibung
	Wenn Sie einen Eintrag bearbeiten, erscheint auf der rechten Seite des Eintrags ein Haken. Klicken Sie auf den Haken, um Ihre Änderungen zu übernehmen.

Bei Site-to-Site-Verbindungen, bei denen Ihre LANCOM R&S®Unified Firewall als Client dient, können Sie die folgenden Elemente konfigurieren:

Eingabefeld	Beschreibung
Adressbereich	Geben Sie den Adressbereich an, aus dem IP-Adressen für diese Verbindung verwendet werden. Der Adressbereich ist in den Einstellungen für VPN-SSL angegeben. Weitere Informationen finden Sie unter *VPN-SSL* auf Seite 37.
Server-Adresse	Geben Sie die IP-Adresse ein, unter der das entfernte Verbindungsende erreichbar ist. Klicken Sie auf **Hinzufügen**, um ein Netzwerk zur Liste hinzuzufügen. Wenn Sie mehr als ein Netzwerk hinzufügen, wird eine automatische Ausfallsicherung ausgelöst, falls das erste Netzwerk nicht erreichbar ist. Ihre LANCOM R&S®Unified Firewall versucht in diesem Fall, nacheinander die übrigen Netzwerke in der Liste zu erreichen, bis ein Netzwerk erreichbar ist. Sie können einzelne Einträge in der Liste bearbeiten oder löschen, indem Sie auf die entsprechende Schaltfläche neben einem Eintrag klicken. Weitere Informationen finden Sie unter *Symbole und Schaltflächen*. Wenn Sie einen Eintrag bearbeiten, erscheint auf der rechten Seite des Eintrags ein Haken. Klicken Sie auf den Haken, um Ihre Änderungen zu übernehmen.
Server-Port	Geben Sie die Port-Nummer ein, die am entfernten Verbindungsende für diese Verbindung verwendet wird.
Verbindungsversuche für	Geben Sie die Zeitüberschreitung in Minuten an, nach deren Ablauf keine weiteren Verbindungsversuche unternommen werden. Wenn diese Option auf 0 eingestellt ist, werden die Verbindungsversuche ohne Unterbrechung fortgesetzt.

Die Schaltflächen rechts unten im Bearbeitungsfeld hängen davon ab, ob Sie eine neue VPN-SSL-Verbindung hinzufügen oder eine bestehende Verbindung bearbeiten. Klicken Sie für eine neu konfigurierte Verbindung auf **Erstellen**, um die Verbindung zur Liste der verfügbaren VPN-SSL-Verbindungen hinzuzufügen, oder auf **Abbrechen**, um Ihre Änderungen zu verwerfen.

Wenn Sie Änderungen vorgenommen haben, können Sie diese mit den Schaltflächen unten rechts im Bearbeitungsfenster speichern (**Speichern**) oder verwerfen (**Zurücksetzen**). Andernfalls können Sie das Fenster schließen (**Schließen**).

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