LANCOM Techpaper
Cloud-managed Security

Netzwerksicherheit ist essenziell für die Geschäftsintegrität – und gleichzeitig ein komplexes Thema: Die steigende Zahl an Cyberangriffen auf Unternehmen und öffentliche Einrichtungen erfordert eine state-of-the-art Security-Architektur, die in vielen Fällen aufwändig und komplex ist. Gleichzeitig werden 99% aller Sicherheitslücken durch Fehlkonfigurationen der eingesetzten Geräte verursacht. Über Cloud-managed Security bzw. Software-defined Security (SD-Security) vereinfachen Sie die Einrichtung und sichern Ihr Netzwerk mit geringem Aufwand professionell ab.

SD-Security – Möglichkeiten und aktuelle Grenzen

Über die im Folgenden beschriebene Einrichtung von SD-Security können Sie mit wenigen Klicks in der LANCOM Management Cloud (LMC) einige Sicherheitsfeatures Ihrer LANCOM R&S®Unified Firewalls bzw. in geringerem Umfang Ihrer LCOS-basierten Router aktivieren.

Mit den LANCOM R&S®Unified Firewalls – entwickelt in Deutschland – erhalten Sie state-of-the-art Unified Threat Management (UTM)-Funktionen für garantiert zuverlässigen Schutz von Netzwerken und Daten. Hier aktivieren Sie den Schutz vor Viren, Malware und Spam ebenso wie die Sicherheit und Integrität Ihrer HTTPS-Verbindungen über SSL Inspection. Letzteres ist auch Voraussetzung für den Content-Filter der LANCOM R&S®Unified Firewalls. Hier muss aktuell noch das Zertifikatsmanagement manuell auf allen Geräten ausgeführt werden.

Über ein Application Management steuern Sie die Applikationsnutzung in Ihrem Netzwerk. Denn Sie wissen am besten, welchen Anwendungen Sie vertrauen und welche Sie unterbinden möchten. Blockieren Sie gezielte einzelne Anwendungen oder Anwendungsgruppen. Leiten Sie von Ihnen bestimmte Anwendungen wie z. B. Microsoft Office 365 direkt ins Internet (Local Internet Breakout) oder zu einer externen Gegenstelle.

Als weiteres Sicherheitsfeature übernimmt die LMC die automatische Einrichtung von VPN-Verbindungen zwischen allen Standorten (Auto-VPN) und Netzwerken (Ende-zu-Ende-VLAN-Übertragung, LANCOM Advanced Routing & Forwarding).

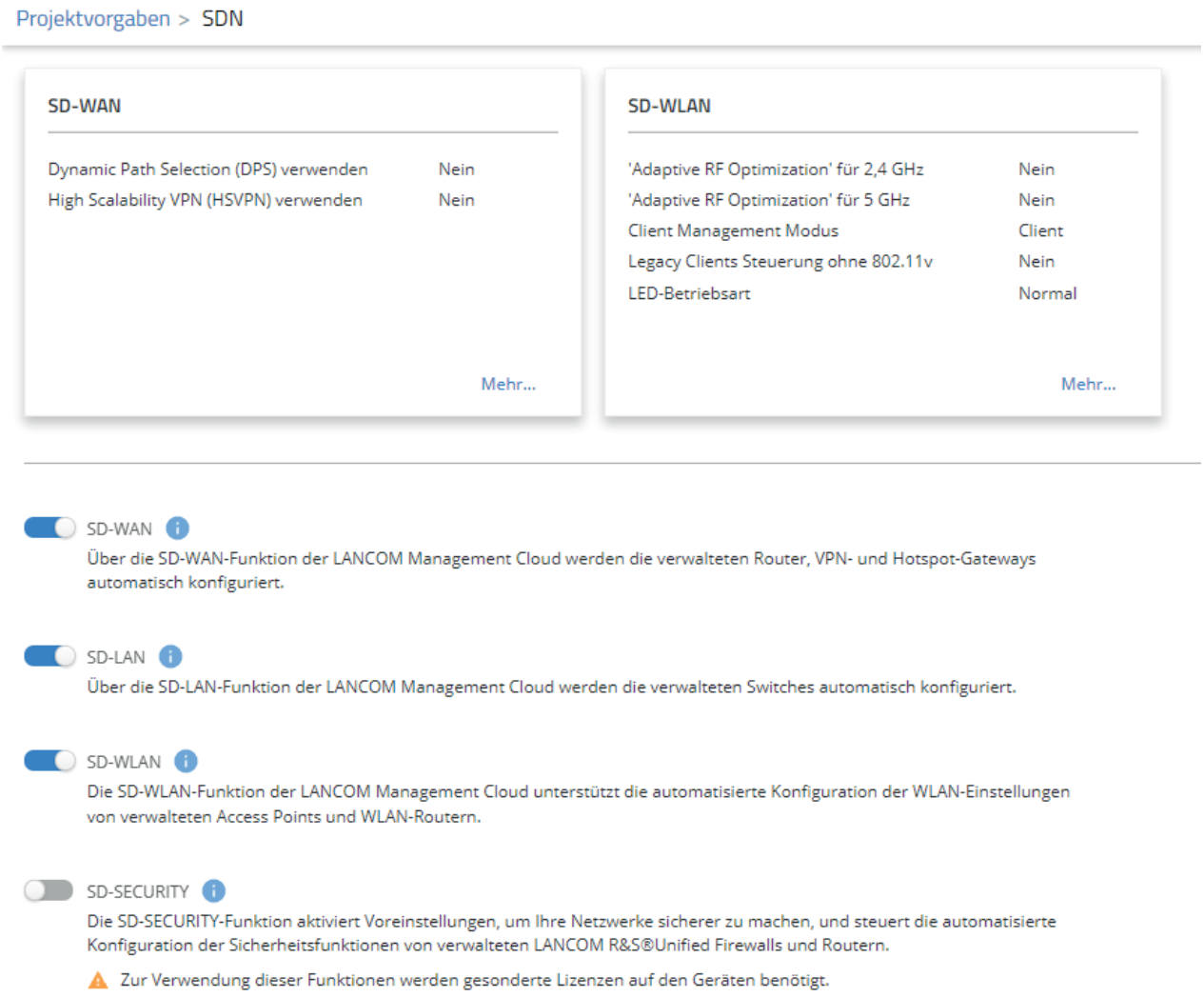
Falls Ihnen diese Möglichkeiten einer SmartConfig noch nicht ausreichen, können Sie bei den LANCOM R&S®Unified Firewalls Port-Filter-Regeln noch manuell einrichten. Nutzen Sie hier entweder die bequem aus der LMC heraus erreichbare Web-Konfigurationsoberfläche oder automatisieren Sie dies über Skripte. Beispiele hierzu finden Sie in unserem Add-In-Handbuch.

LANCOM Systems

SD-Security in der LANCOM Management Cloud (LMC) einrichten

Führen Sie die folgenden Schritte zur Aktivierung von SD-Securtiy in der LMC aus:

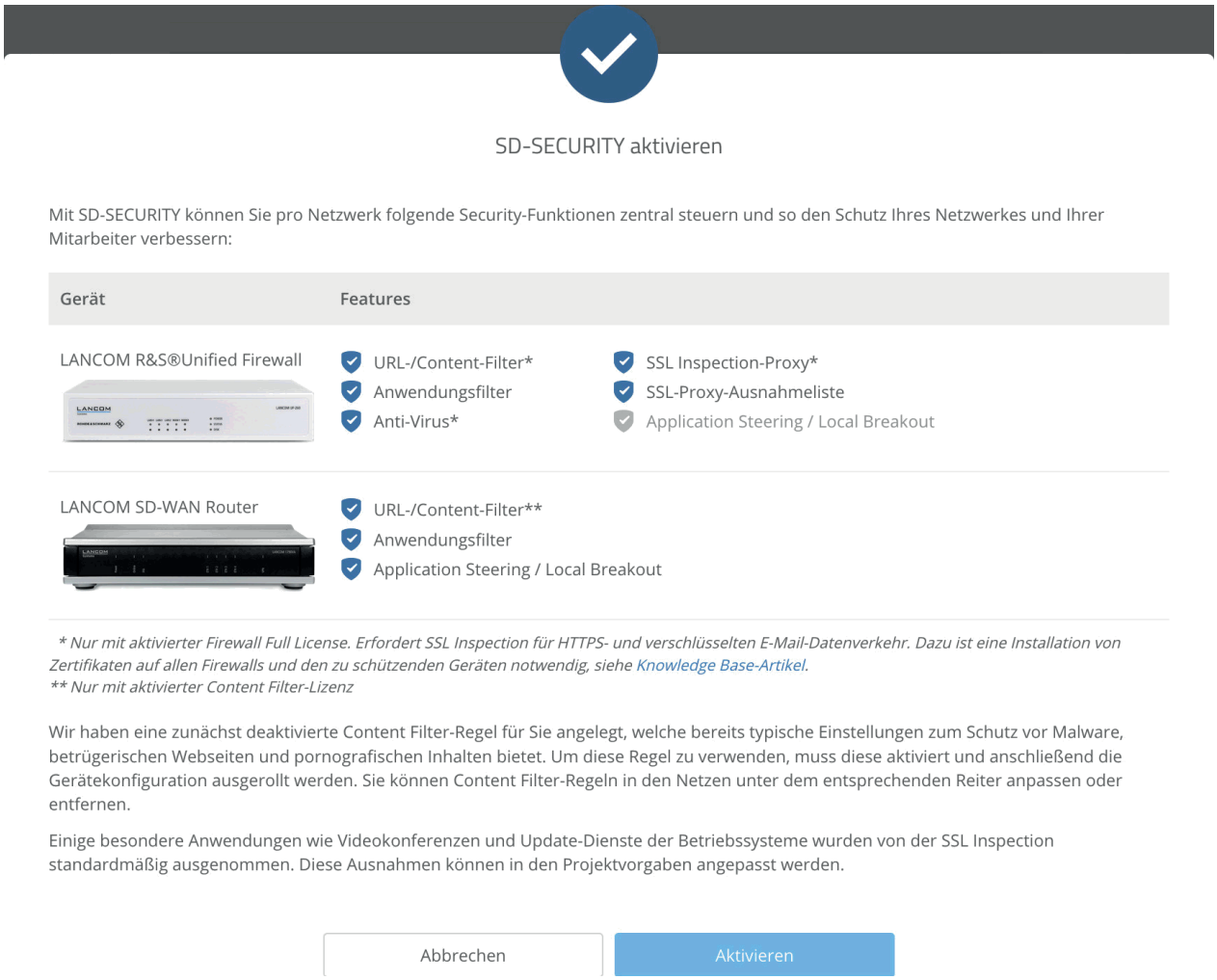
1. Melden Sie sich in der LMC an.
2. Überprüfen sie in den unter **Projektvorgaben > SDN**, ob das Feature **SD-Security** aktiv ist.



Aktivieren Sie ggf. **SD-Security**.

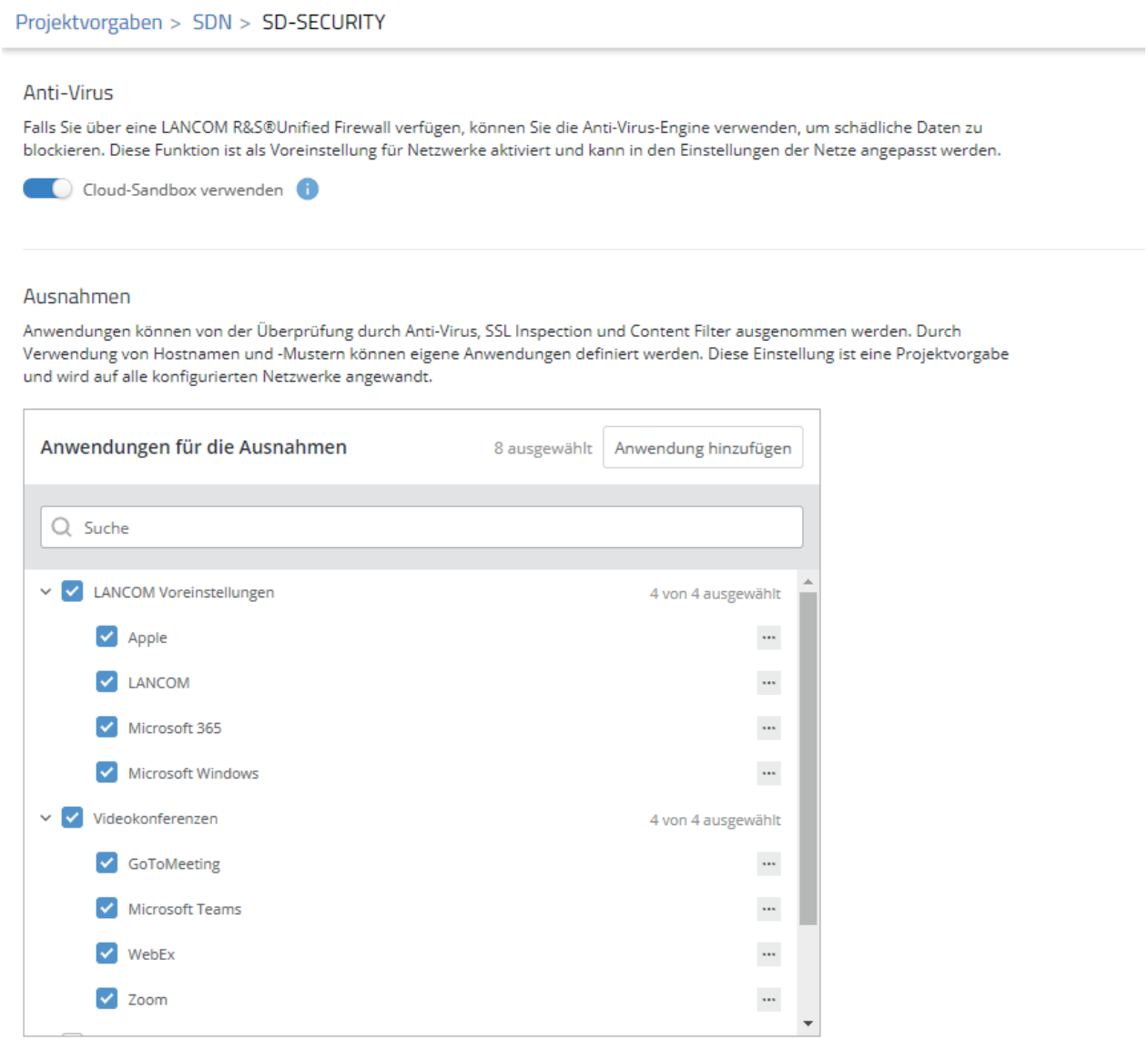
Zur Verwendung dieser Funktionen benötigt jedes Gerät eine eigene Lizenz! Für LANCOM R&S®Unified Firewalls ist dies eine Full License, für LCOS-basierte Router die Content-Filter-Option. Diese müssen im Vorfeld bereits manuell auf den Geräten eingespielt werden.
Pro Gerät muss außerdem in der LMC eine LMC-Lizenz aktiv sein.

Es öffnet sich ein Fenster mit Informationen zu SD-Security.



Im Anschluss können Sie SD-Security **aktivieren** oder ggf. die Aktivierung abbrechen.

3. Überprüfen Sie die Standardeinstellungen von SD-Security unter **Projektvorgaben > SDN > SD-Security** und passen Sie diese ggf. an.



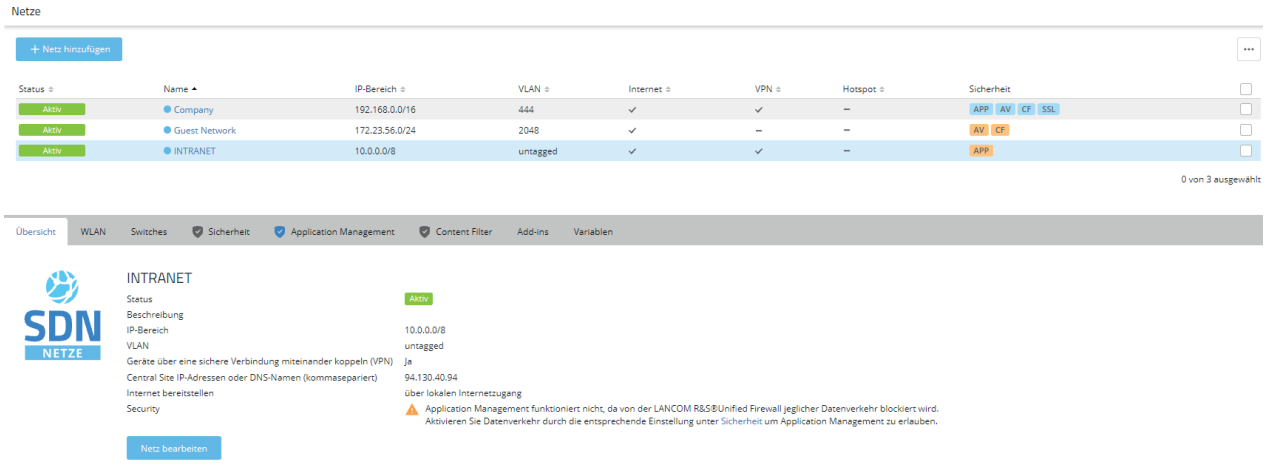
› Aktivieren Sie ggf. die Verwendung der **Cloud-Sandbox**.
Die Cloud-Sandbox erweitert den Anti-Virus-Schutz und ist nur auf Netzen aktiv, wo der Anti-Virus-Schutz aktiv ist. Zum Schutz vor noch nicht bekannten Bedrohungen kann die LANCOM R&S®Unified Firewall verdächtige Dateien in eine geschützte Cloud hochladen. In dieser getrennten Umgebung werden sie per Machine Learning und Sandboxing sicher und zuverlässig getestet.

Wenn Sie die Cloud-Sandbox aktivieren, dann werden die **Machine Learning-Funktionen** ebenfalls aktiviert.

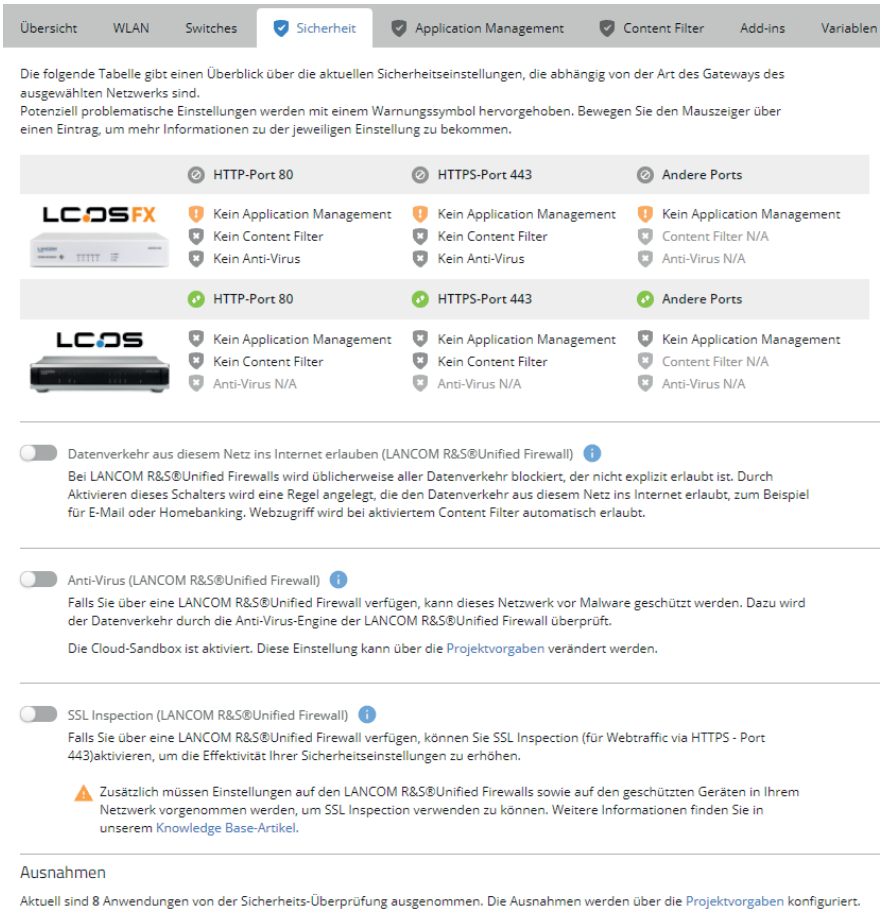
› Überprüfen Sie die Ausnahmelisten, ob für Ihr Netzwerk noch ein Service eingetragen oder abgewählt werden muss.

4. In der Rubrik **Netze** haben Sie jetzt zusätzliche Einstellungen zur Verfügung, um weitere Security-Features zu aktivieren.

   Unter der Netzwerkdefinition – z. B. INTRANET – finden Sie jetzt zusätzliche Tabs:



› Tab **Sicherheit**



i. In der Übersicht sehen Sie, welche Sicherheitsfunktionen Sie für welches LANCOM Produkt aktiviert haben. Ein Mouse-Hover-Effekt über den Icons liefert Ihnen weitere Informationen.
ii. Datenverkehr aus diesem Netz ins Internet erlauben (LANCOM R&S®Unified Firewall)
Diese Option erlaubt den vollständigen Zugriff auf das Internet (Pass-All). Alternativ können Sie über das Web-Interface der LANCOM R&S®Unified Firewall eine detailliertere Konfiguration vornehmen.
iii. Anti-Virus (LANCOM R&S®Unified Firewall)
Datenverkehr zwischen diesem Netzwerk und dem Internet kann durch die Anti-Virus-Engine der LANCOM R&S®Unified Firewalls geleitet werden, um verdächtige Dateien zu entdecken und zu blockieren, bevor sie in Ihr Netzwerk gelangen.
Um auch verschlüsselten Datenverkehr überprüfen zu können, muss zusätzlich SSL Inspection aktiviert und eingerichtet werden.
iv. SSL Inspection (LANCOM R&S®Unified Firewall)
Falls Sie über eine LANCOM R&S®Unified Firewall verfügen, können Sie SSL Inspection aktivieren, um auch verschlüsselten Datenverkehr zu kontrollieren und somit die Effektivität Ihrer Sicherheitseinstellungen zu erhöhen. Diese Einstellung ist pro Netzwerk verfügbar und kann daher in den Einstellungen der Netze angepasst werden.

UTM-Features wie Anti-Virus und Content-Filter setzen eine SSL Inspection voraus. Wenn SSL Inspection in der LANCOM R&S®Unified Firewall aktiv ist, dann leitet die LANCOM R&S®Unified Firewall HTTPS-Verbindungen auf sich selbst um und fungiert als Proxy zwischen Endgerät und Server. Das Endgerät muss das explizit akzeptieren, indem es der Proxy Certificate Authority der LANCOM R&S®Unified Firewall vertraut.

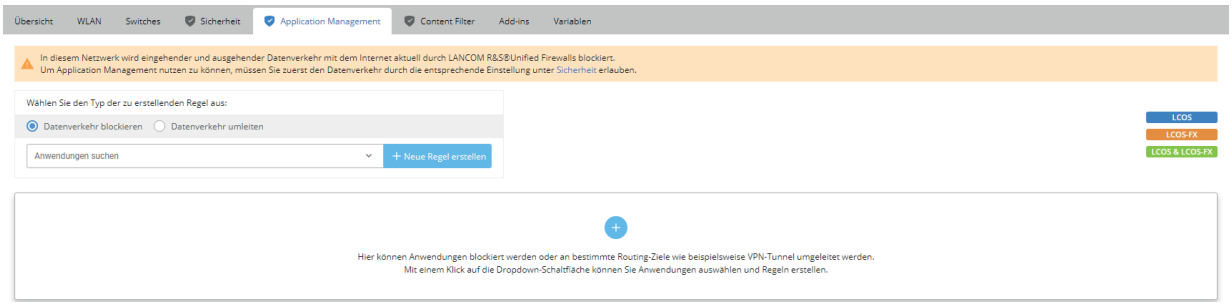
Notwendige manuelle Einrichtung von Zertifikaten auf den LANCOM R&S®Unified Firewalls bei SSL Inspection

Bei mehreren LANCOM R&S®Unified Firewalls an mehreren Standorten existieren zwei Möglichkeiten:

a. CA pro Firewall: Jede LANCOM R&S(R)Unified Firewall hat eine unabhängige Proxy Certificate Authority
b. Firmenweite CA: Vertraut ein Endgerät einer vorab angelegten und übergeordneten CA, lässt sich dieses ohne weiteren Aufwand an allen Standorten nutzen

Beide Fälle sind in unserem Knowledge Base-Artikel beschrieben, wobei die LMC Ihnen bereits einige der dort beschriebenen Schritte abnimmt. Es bleibt allerdings noch die Installation der Zertifikate, welche manuell erfolgen muss.

Tab **Application Management**



Wir unterscheiden beim Application Managment drei Rubriken:

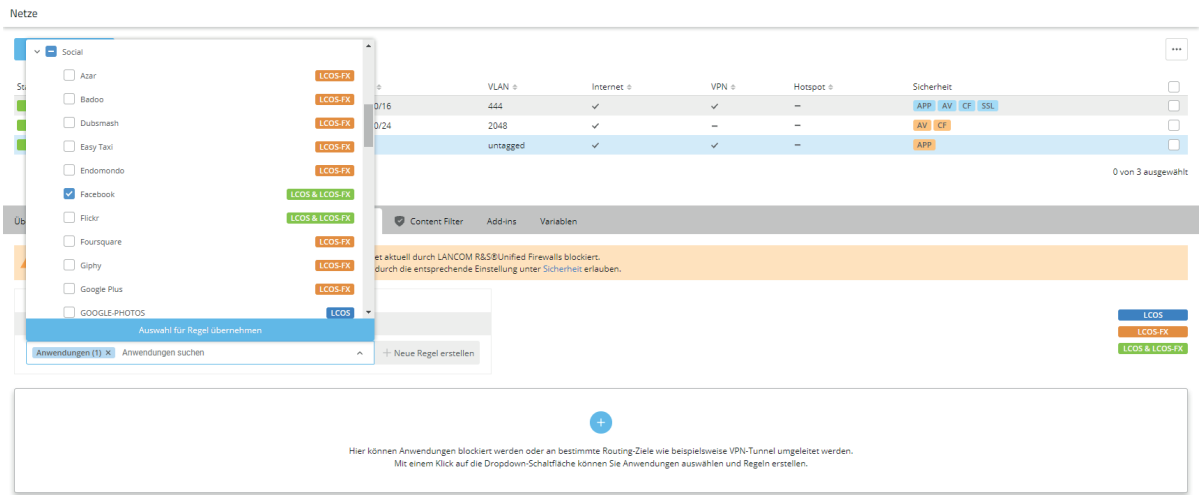
LCOS (Blau)	LCOS-basierte Geräte (Router) wie z. B. LANCOM 1926VA
LCOS FX (Orange)	LANCOM R&S®Unified Firewalls
LCOS & LCOS FX (Grün)	LCOS-basierte Geräte (Router) und LANCOM R&S®Unified Firewalls

Mit dieser Information können Sie überprüfen, welcher Service von Ihrem Gerät erkannt wird.

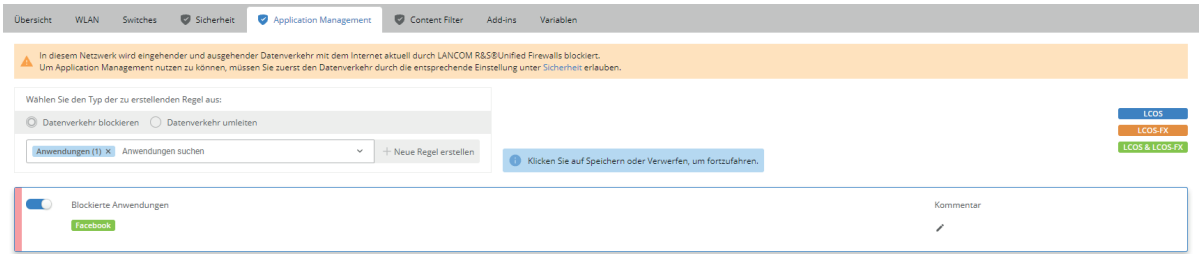
Sie können den Datenverkehr entweder blockieren oder umleiten:

i. Datenverkehr blockieren

Sie können den Traffic wie z. B. zu „Facebook“ sehr leicht für ein Netz blockieren: Wählen Sie im oberen Bereich des Application Management die Checkbox **Datenverkehr blockieren** aus. Anschließend klicken Sie auf die Schaltfläche **Neue Regel erstellen** und in dem neu erscheinenden Dialog können Sie einen oder mehrere Services auswählen.



Übernehmen Sie Ihre Auswahl über die Schaltfläche **Auswahl für Regel übernehmen**. Eine erstellte Regel wird standardmäßig aktiviert.



In diesem Netzwerk wird eingehender und ausgehender Datenverkehr mit dem Internet aktuell durch LANCOM R&S®Unified Firewalls blockiert. Um Application Management nutzen zu können, müssen Sie zuerst den Datenverkehr durch die Einstellung der Option **Datenverkehr aus diesem Netz ins Internet erlauben (LANCOM R&S®Unified Firewall)** auf dem Tab **Sicherheit** erlauben.

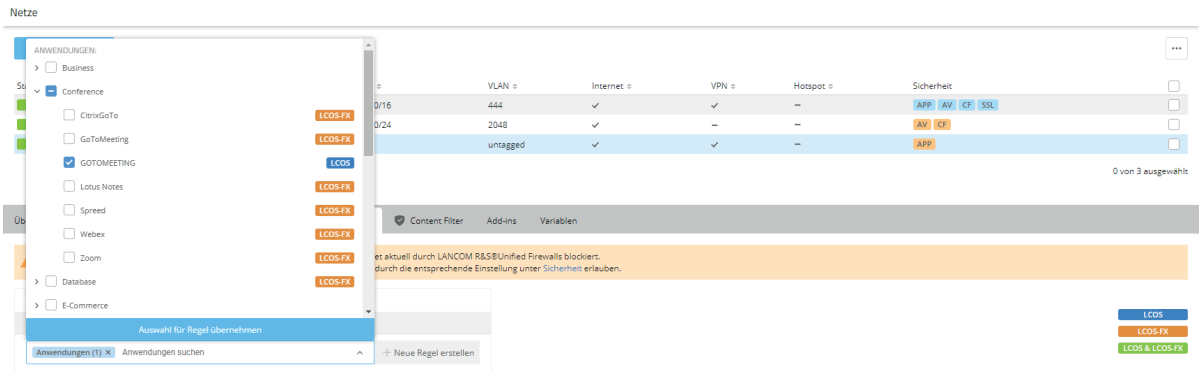
ii. Datenverkehr umleiten

Wählen Sie im oberen Bereich des Application Management die Checkbox **Datenverkehr umleiten** aus.

Das Umleiten von Anwendungen wird zum Zeitpunkt der Erstellung dieses Dokuments nur von LCOS-basierten Geräten unterstützt. Die Funktion wird für LCOS FX basierte Firewalls bis Ende 2021 bereitgestellt. Zeitkritische Anwendungen werden bei LCOS FX bis dahin vom SSL Proxy ausgenommen, aber aktuell noch ohne Local Internet Breakout weitergeleitet.

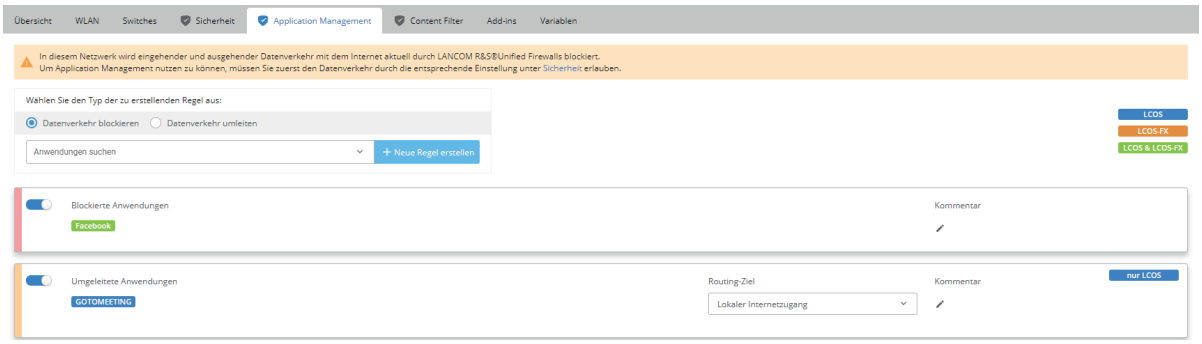
Die LANCOM R&S®Unified Firewall kann auch Anwendungen und/oder Protokolle umleiten. Dieses müssen Sie über die Weboberfläche manuell einstellen.

Sie können den Traffic wie z. B. zu dem Konferenzdienst „GoToMeeting" sehr leicht für ein Netzwerk umleiten. Dafür klicken Sie auf die Schaltfläche **Neue Regel erstellen** und in dem neu erscheinenden Dialog können Sie einen oder mehrere Services auswählen.

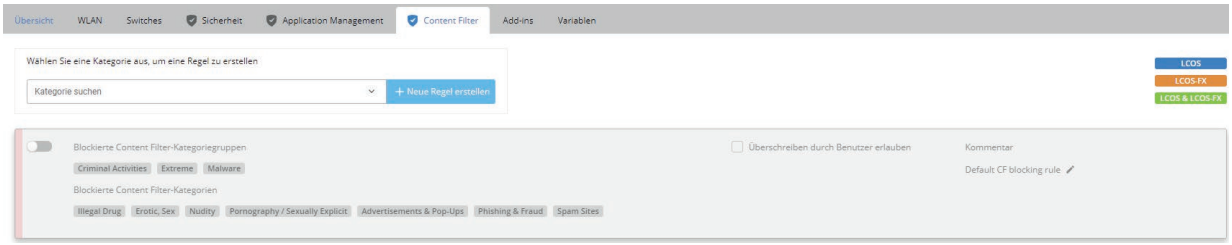


Sie müssen sich entscheiden, wie Sie den Traffic umleiten wollen. Dieses können Sie im Dropdown Menü **Routing-Ziel** machen.

Wenn Sie z. B. bei einem Netzwerk ausgewählt haben, dass der komplette Traffic über das Central Site Gateway geroutet werden soll, können Sie einzelne Anwendungen direkt über einen vorhandenen lokalen Internetzugang routen lassen (Local Internet Breakout).



› Tab **Content Filter**



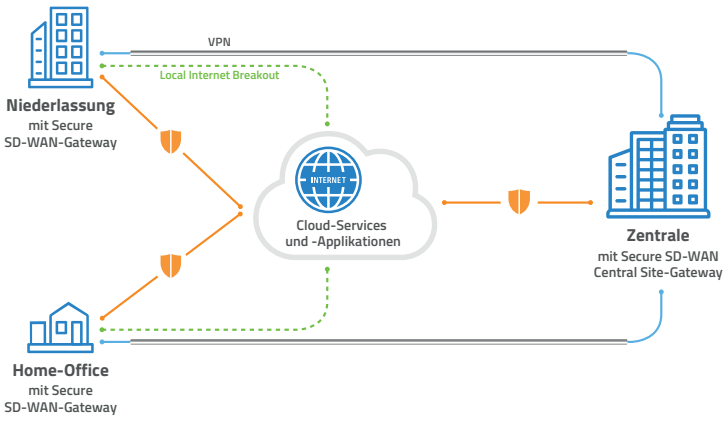
i. In diesem Bereich können Sie die Content Filter-Regeln sowohl für die LANCOM R&S®Unified Firewalls als auch für LCOS-basierte Router einstellen. Als Beispiel haben wir Ihnen eine „Default CF blocking rule“ zur Verfügung gestellt. Damit Sie unsere Beispielregel testen können, müssten Sie diese nur aktivieren.

5. Sobald alle Einstellungen korrekt gesetzt sind und sowohl die Netze als auch Geräte dem Standort zugewiesen sind, können Sie diese Konfigurationsänderungen ausrollen.

Beispielhafte Einsatzszenarien

Szenario 1: Dezentrale Security an allen Standorten

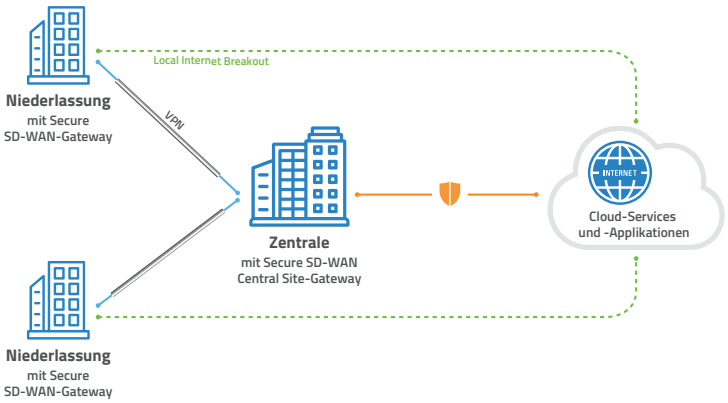
In diesem Szenario werden alle Niederlassungen per SD-WAN/Auto-VPN an die Zentrale für einen sicheren Zugriff auf zentral gehostete Ressourcen und Dienste angebunden. Dabei kommt an jedem Standort ein Gateway mit voll aktivierten Security-Funktionen zum Einsatz, womit die Sicherheitsvorgaben pro Standort individuell definiert werden. Zudem werden durch den Einsatz eines lokalen Internet Breakouts zur Nutzung von vertrauenswürdigen Cloud-basierten Anwendungen die Latenzzeiten für die Benutzer sehr gering gehalten. Dieses Szenario dürfte die meisten Standardfälle abdecken.



Empfehlung: Setzen Sie an jedem Standort eine lokale LANCOM R&S®Unified Firewall ein. Dadurch erreichen Sie eine maximale Performance durch den jeweils lokalen Internetzugang bei gleichzeitig hoher Sicherheit durch die Firewall.

Szenario 2: Zentrale Security

Dieses Szenario ist ideal und kosteneffizient für kleinere Filialvernetzungsszenarien. Auch hierbei werden alle Niederlassungen per SD-WAN/Auto-VPN an die Zentrale für einen sicheren Zugriff auf zentral gehostete Ressourcen und Dienste angebunden. Dabei kommt in der Zentrale ein leistungsstarkes Gateway mit voll aktivierten Security-Funktionen zum Einsatz, welches die Sicherheitsvorgaben für alle Niederlassungen vorgibt. In den Niederlassungen genügt der Einsatz kleinerer SD-WAN-Gateways ohne aktivierte Security-Funktionen, wobei ein Local Internet Breakout für vertrauenswürdige Cloud-Anwendungen die Traffic-Last auf der Zentralseite reduzieren kann.



Dieses Szenario ist insbesondere für Fälle geeignet, in denen der lokale Internetzugang eine untergeordnete Rolle spielt oder nicht erforderlich ist, wenn z. B. an den jeweiligen Standorten Maschinen angeschlossen werden sollen.

Szenario 3: Kleine Netze – Gleichberechtigte Standorte ohne Zentrale

Bei Unternehmensnetzwerken ohne klassische Zentrale sind alle Standorte untereinander komplett via Auto-VPN vernetzt. Dabei kommt an allen Standorten ein Gateway mit aktivierten Security-Funktionen zum Einsatz. Die Standorte greifen jeweils gleichberechtigt auf lokal gehostete Dienste an allen Standorten zu. Die Sicherheitsvorgaben können auch hier pro Standort individuell definiert werden, ebenso wie der Local Internet Breakout für vertrauenswürdige Cloud-Anwendungen.