Cloud-managed Security

Netzwerksicherheit ist essenziell für die Geschäftsintegrität – und gleichzeitig ein komplexes Thema: Die steigende Zahl an Cyberangriffen auf Unternehmen und öffentliche Einrichtungen erfordern ein dynamisches Sicherheitskonzept, das auf neuartige Bedrohungen reagieren kann. Trotz einer state-of-the-art Security-Architektur können vereinzelte Fehlkonfigurationen eingesetzter Geräte große Sicherheitslücken zur Folge haben. Über Cloud-managed Security vereinfachen Sie die Einrichtung und sichern Ihr Netzwerk mit geringem Aufwand professionell ab.

Erfahren Sie in diesem Paper, wie Sie Sicherheitsprofile für alle Geräte eines Netzwerkes zentral über die LANCOM Management Cloud (LMC) einrichten und welche Security-Architektur für Ihr Einsatzszenario geeignet ist.

Was ist Cloud-managed Security?

Von über die Cloud verwalteter Sicherheit spricht man, wenn Sicherheitsfunktionen von der Hardware, also z. B. Firewalls, abstrahiert werden und auf eine Software-Ebene verlagert werden. Die Sicherheitsinfrastruktur wird somit virtualisiert kontrolliert und gesteuert. Ein Management-System, das die Funktionen sicher und zentral verwaltet, kann zum Beispiel die LANCOM Management Cloud (LMC) sein.

Cloud-managed Security mit der LMC – automatisiert. sicher. zentral.

Mit der LANCOM Management Cloud (LMC) verwalten, steuern und optimieren Sie Ihre gesamte Netzwerkarchitektur in den Bereichen WAN, LAN, WLAN und Security. Im Zusammenspiel mit den LANCOM R&S®Unified Firewalls bzw. den LCOS-basierten Routern und SD-WAN Gateways aktivieren Sie mit nur wenigen Klicks Sicherheitsfunktionen für den garantiert zuverlässigen Schutz von Netzwerken, Geräten und Daten. Entwickelt in Deutschland und ausgestattet mit state-of-the-art Unified Threat Management (UTM)-Funktionen bieten die LANCOM R&S®Unified Firewalls beispielsweise höchste Sicherheit und Integrität Ihrer HTTPS-Verbindungen über SSL Inspection. Mit Hilfe eines Content Filters können jugendgefährdende als auch geschäftsgefährdende Inhalte zielsicher blockiert werden.

Und damit nicht genug: 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).

All diese Sicherheitsfunktionen behalten Sie übersichtlich unter dem Menüpunkt ‚Sicherheit' im Auge. Für die Einrichtung und Konfiguration der dafür notwendigen Sicherheitsprofile in der LMC unterstützt Sie die folgende Schritt-für-Schritt-Anleitung.

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

Führen Sie die folgenden Schritte zur Aktivierung der Sicherheitseinstellungen in der LMC aus:

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

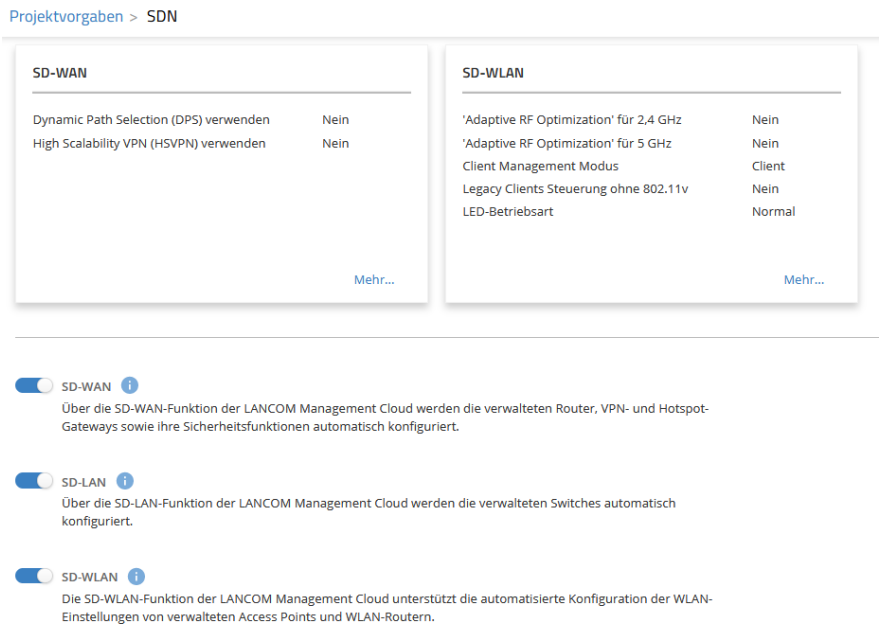

Abbildung 1:
Projektvorgaben > SDN

Aktivieren Sie ggf. **SD-WAN**. Daraufhin erscheint im Menü ein zusätzlicher Eintrag ‚Sicherheit'.

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 und SD-WAN Gateways die LANCOM 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.

3. Unter **Sicherheit > Profile** wird für jedes Netz automatisch ein Sicherheitsprofil mit Standardeinstellungen angelegt. In der Übersicht behalten Sie die eingestellten Sicherheitsfunktionen im Blick.

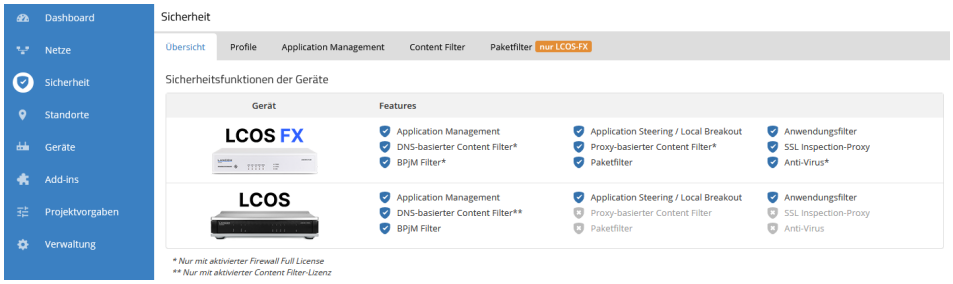

Abbildung 2: Übersicht der Sicherheits-funktionen

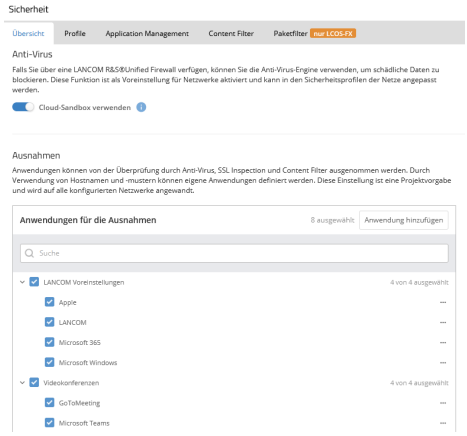

Abbildung 3: Standardeinstellungen der Sicherheitsprofile

Aktivieren Sie ggf. die Verwendung der **Cloud-Sandbox**.
Die Cloud-Sandbox erweitert den Anti-Virus-Schutz und ist nur auf Netzen aktiv, bei denen 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. Erfahren Sie mehr dazu in unserem Infopaper Avira Protection Cloud.

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. Sie können jetzt global für alle Netze Regeln in den Tabs **Application Management**, **Content Filter** und **Paketfilter** nach Ihrem Bedarf anlegen und justieren. Diese können Sie im Anschluss auf Ihre Netze / Sicherheitsprofile anwenden.

   - Tab **Application Management**

   Wir unterscheiden beim Application Managment drei Rubriken:

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

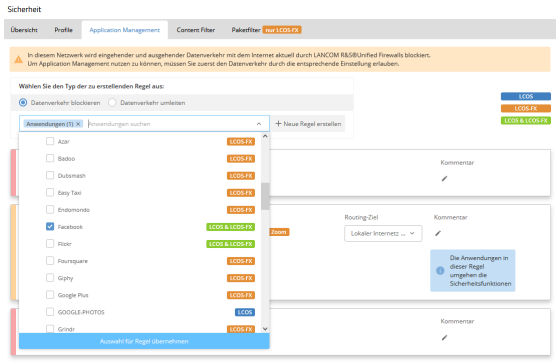

Abbildung 4: Datenverkehr blockieren

   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)** erlauben. Dies nehmen Sie in den zuvor erwähnten allgemeinen Einstellungen eines Sicherheitsprofiles vor.

ii) Datenverkehr umleiten

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

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.

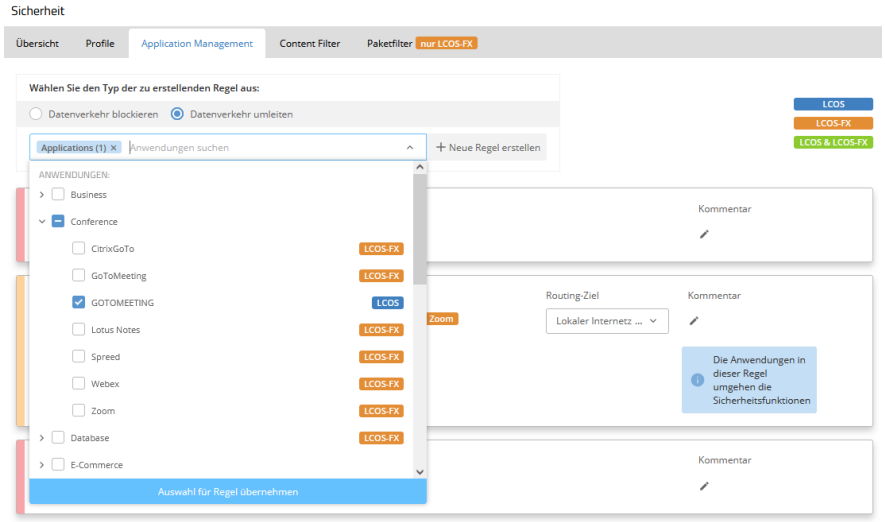

Abbildung 5:
Datenverkehr umleiten

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**

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

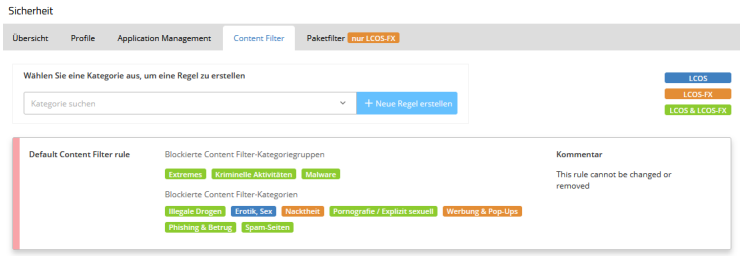

Abbildung 6:
Tab Content Filter

- Tab **Paketfilter**

In diesem Bereich können Paketfilter-Regeln erstellt werden, die in einem Sicherheitsprofil verwendet werden können. Wählen sie zunächst eine Aktion (verbieten oder erlauben) und eine Richtung des Datenverkehrs (nur ausgehend, nur eingehend oder bidirektional). Im Feld „Ziel“ können Sie ein oder mehrere Ziele für den Datenverkehr definieren, z.B. allgemeine Ziele wie „Internet“ oder „Jedes Ziel“ oder bestimmte Netzwerke. Die Quelle des Datenverkehrs wird automatisch durch das Sicherheitsprofil bestimmt, in dem Sie diese Regel verwenden. Im letzten Schritt können Sie die Regel noch weiter verfeinern, indem Sie Protokolle und Portnummern angeben. Dabei sind Komma-separierte Aufzählungen und mit Bindestrich gekennzeichnete Netzwerkbereiche möglich; diese dürfen sich aber nicht überlappen.

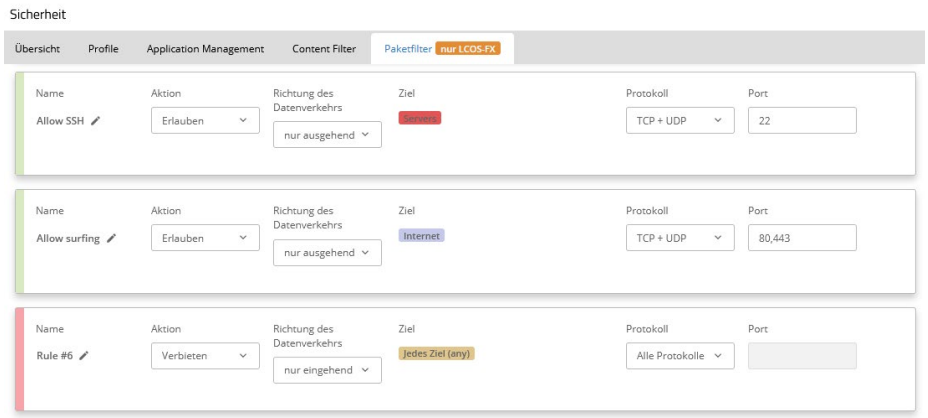

Abbildung 7:
Tab Paketfilter

- **Allgemeine Einstellungen**

Sie erreichen die allgemeinen Einstellungen eines Sicherheitsprofiles mit Klick auf den entsprechenden Namen Ihres Netzes unter **Sicherheit > Profile**.

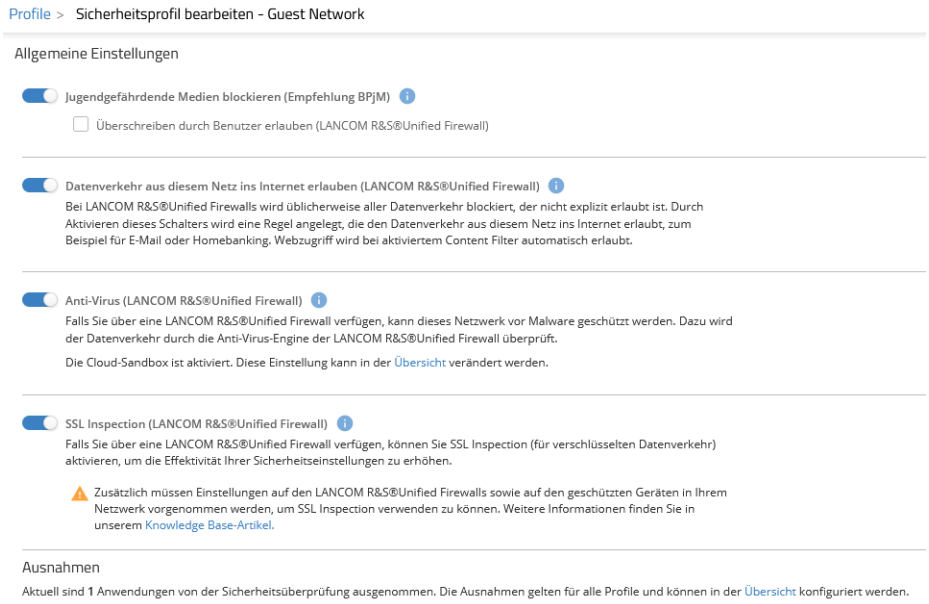

Abbildung 8:
Allgemeine Einstellungen

i) **Jugendgefährdende Medien blockieren (Empfehlung BPjM)**
Diese Option aktiviert den LANCOM BPjM-Filter als Content Filter mit einer offiziellen Webseiten-Liste der Bundesprüfstelle für jugendgefährdende Medien (BPjM). Diese Filterliste sperrt Domains, deren Inhalte offiziell als jugendgefährdend eingestuft werden.

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.

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®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.

5. Die von Ihnen eingestellten Sicherheitsfunktionen können sie für jedes Sicherheitsprofil, also für jedes Ihrer Netze, unter **Sicherheit > Profile** einsehen.

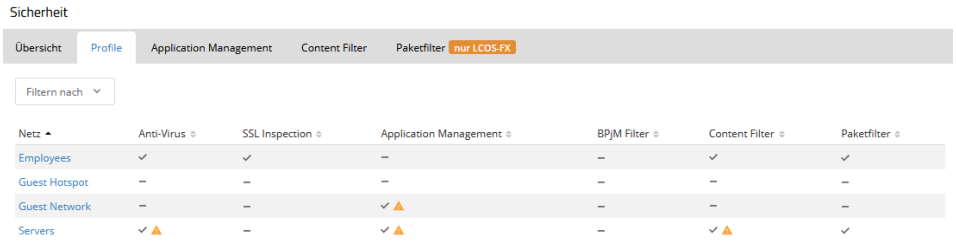

Abbildung 9: Sicherheitsprofile

Beispielhafte Einsatzszenarien

Eine Security-Infrastruktur sollte konkret auf Ihre Unternehmensgröße und die Auslastung Ihres Netzwerkes angepasst und abgestimmt sein, um Sicherheitsvorgaben Ihrem Bedarf anzupassen. So ergeben sich die folgenden drei Szenarien:

Szenario 1: Dezentrale Security an allen Standorten

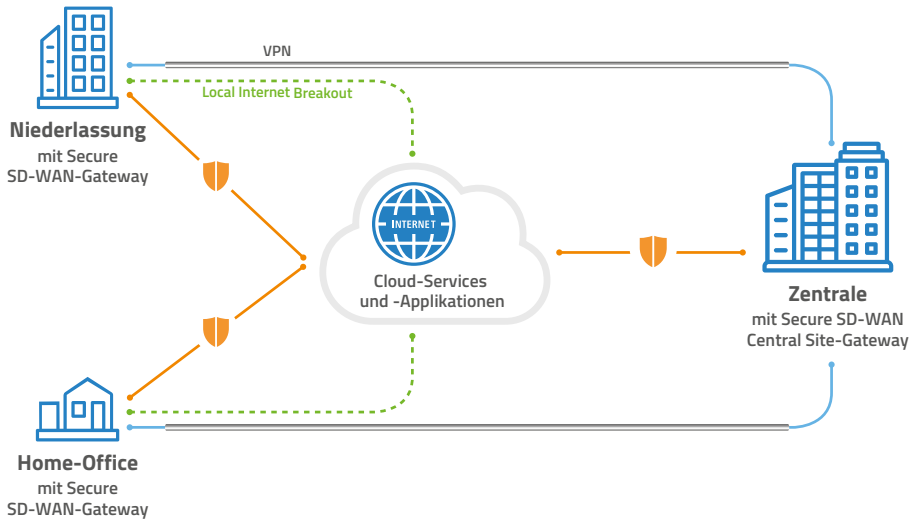

Abbildung 10: Szenario 1: Dezentrale Security an allen Standorten

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

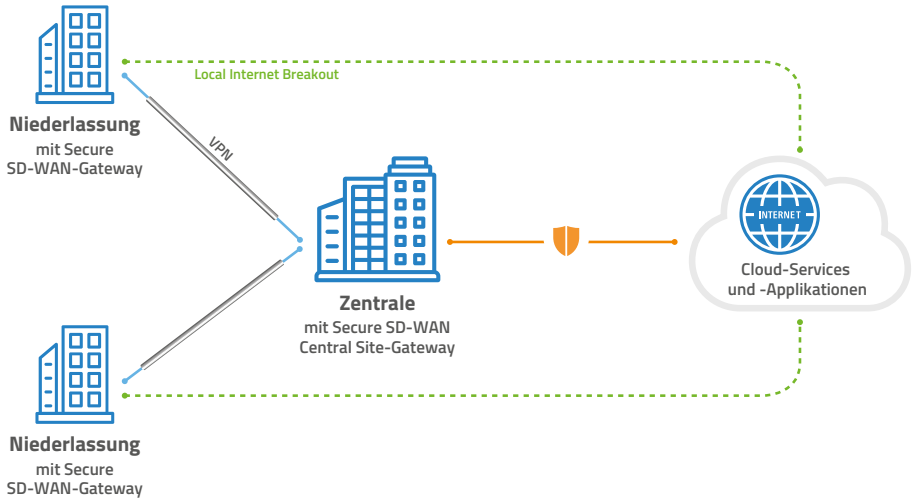

Abbildung 11:
Szenario 2:
Zentrale Security

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

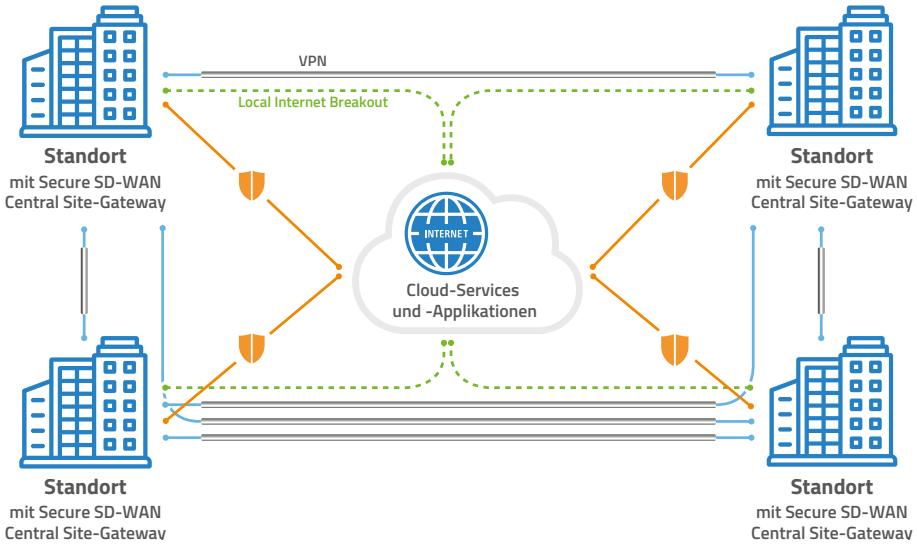

Abbildung 12:
Szenario 3: Kleine Netze – Gleichberechtigte Standorte ohne Zentrale

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.

LANCOM Systems GmbH
Adenauerstr. 20/B2
52146 Würselen | Deutschland
info@lancom.de
www.lancom-systems.de