LANCOM Techpaper
Cloud-managed Security

Network security is essential for business integrity—and at the same time a complex topic: The increasing number of cyber attacks on companies and public institutions requires a state-of-the-art security architecture, which in many cases is costly and complex. At the same time, 99% of all security breaches are caused by misconfigurations of the devices used. With cloud-managed security or software-defined security (SD-Security), you simplify the setup and secure your network professionally with little effort.

SD-Security – possibilities and current limits

Using the setup of SD-Security described below, you can activate some security features of your LANCOM R&S®Unified Firewalls or, to a lesser extent, of your LCOS-based routers in the LANCOM Management Cloud (LMC) with just a few clicks.

With the LANCOM R&S®Unified Firewalls—developed in Germany—you get state-of-the-art Unified Threat Management (UTM) functions for guaranteed reliable protection of networks and data. Here you activate protection against viruses, malware, and spam as well as the security and integrity of your HTTPS connections via SSL inspection. The latter is also a prerequisite for the Content Filter of the LANCOM R&S®Unified Firewalls. Currently, certificate management still has to be performed manually on all devices.

Application management lets you control application usage on your network. Because you know best which applications you trust and which you want to prevent. Block specific individual applications or groups of applications. Route applications you specify, such as Microsoft Office 365, directly to the Internet (Local Internet Breakout) or to an external remote site.

As an additional security feature, the LMC handles the automatic establishment of VPN connections between all sites (Auto-VPN) and networks (end-to-end VLAN transmission, LANCOM Advanced Routing & Forwarding).

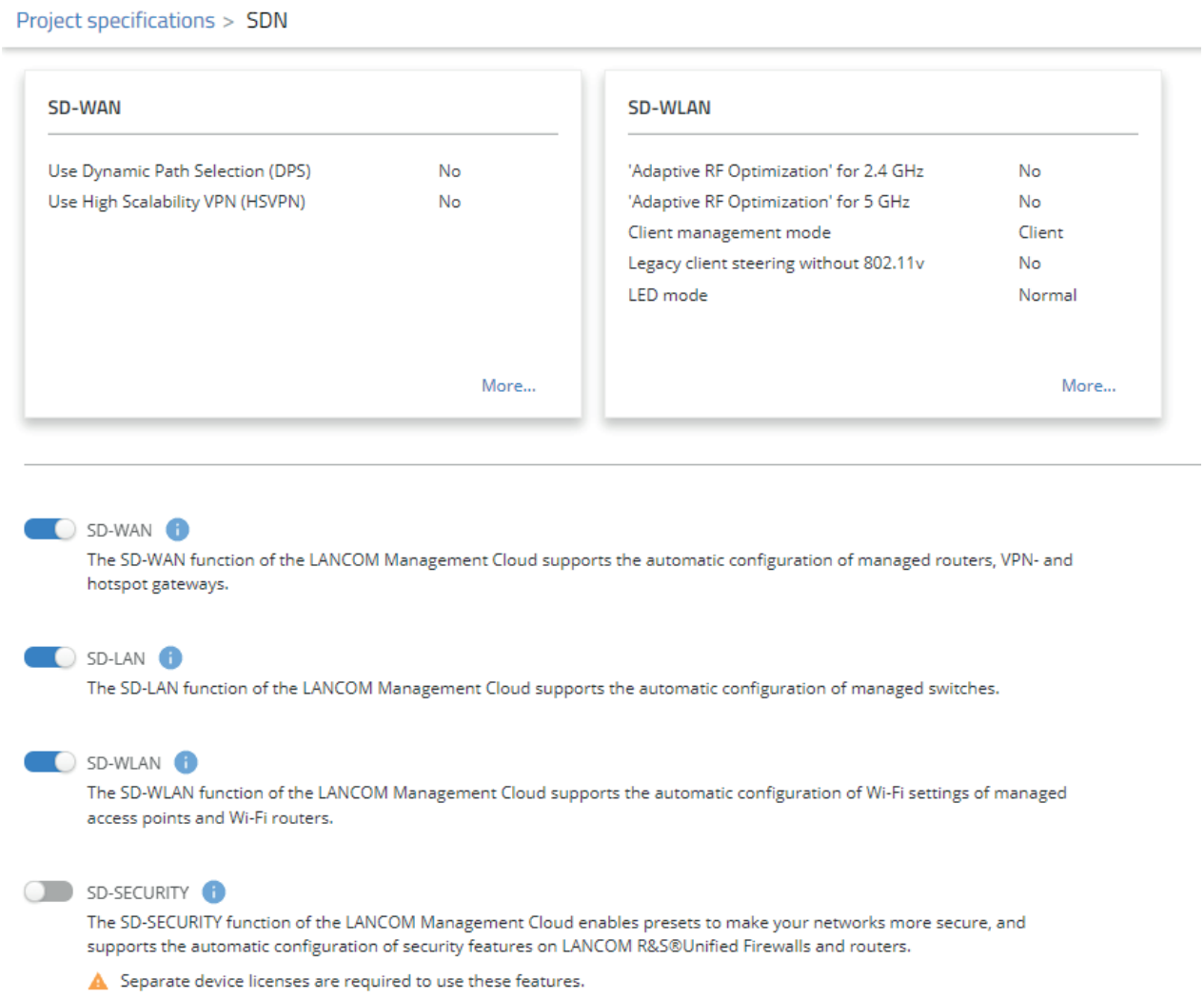
If these SmartConfig options are not enough for you, you can still set up port filter rules manually for the LANCOM R&S®Unified Firewalls. You can either use the Web configuration interface, which is easily accessible from the LMC, or you can automate this process using scripts. Examples of this can be found in our add-in manual.

LANCOM
Systems

Setting up SD-Security in the LANCOM Management Cloud (LMC)

Perform the following steps to enable SD Security in the LMC:

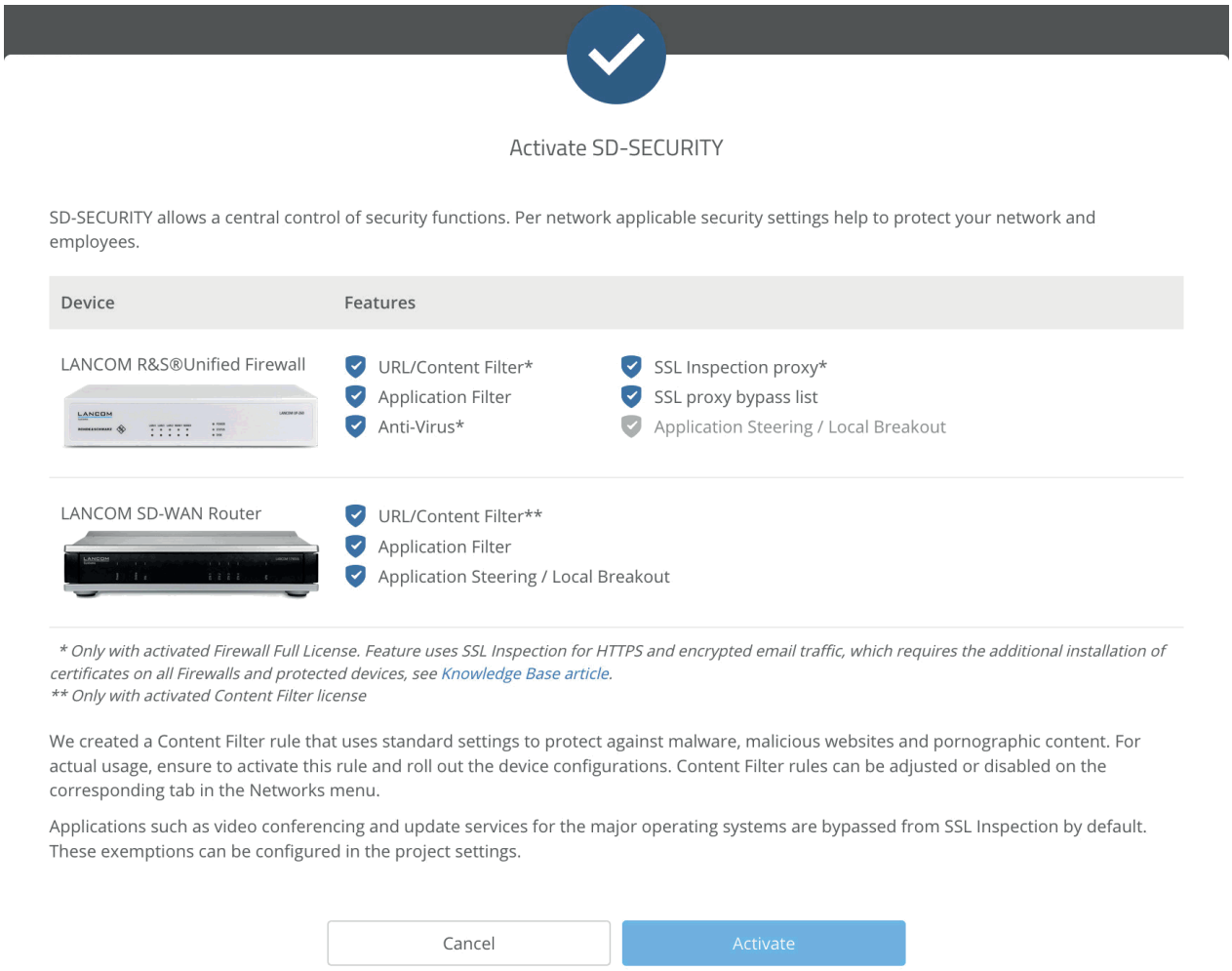
1. Log in to the LMC.
2. Check whether the **SD-Security** feature is active in the **Project specifications > SDN**.



Activate **SD-Security** if necessary.

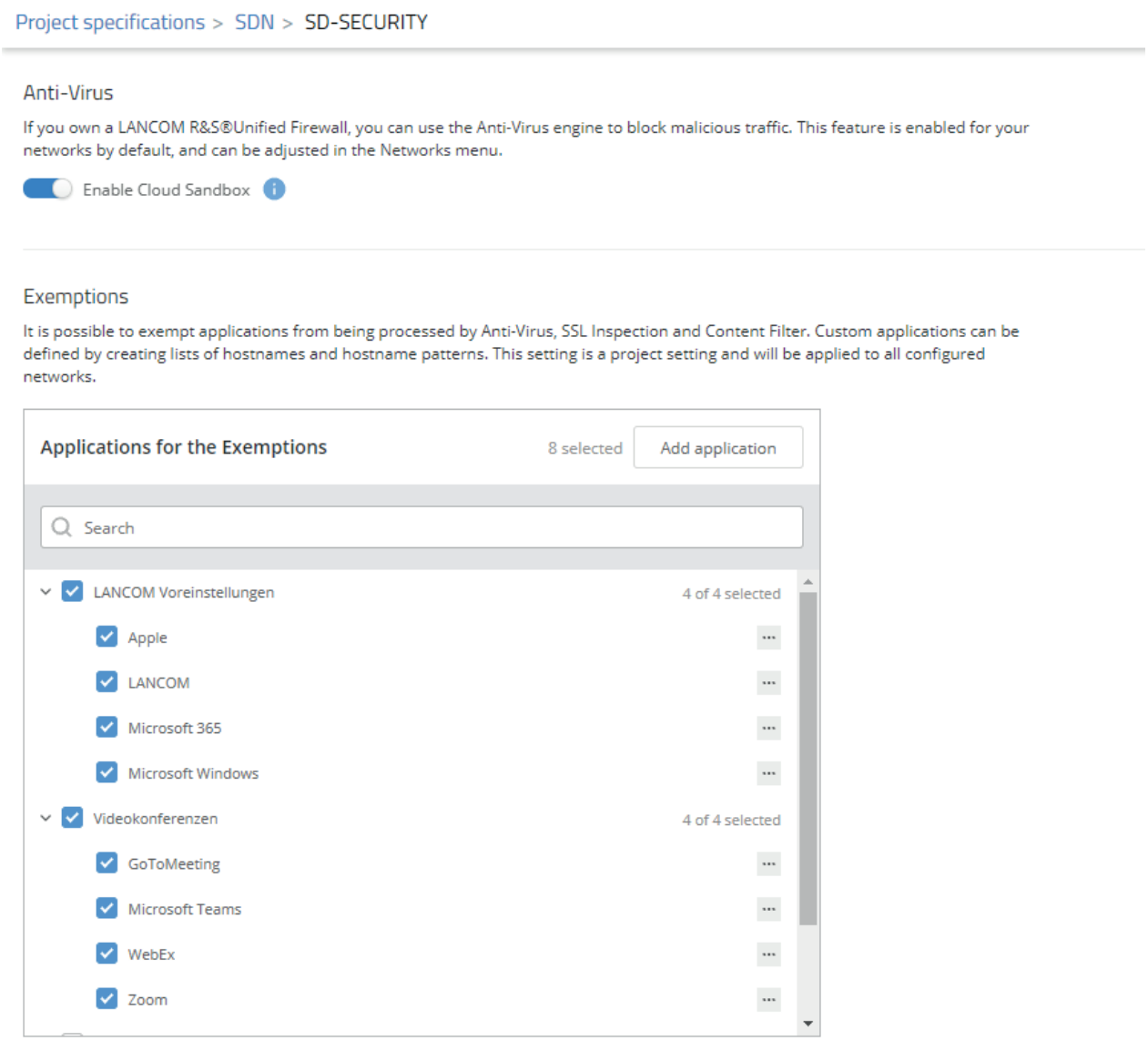
To use these functions, each device requires its own license! For LANCOM R&S®Unified Firewalls this is a Full License, for LCOS-based routers the Content Filter option. These must be manually installed on the devices in advance.
One LMC license must also be active in the LMC for each device.

A window opens with information about SD-Security.



Afterwards, you can **activate** SD-Security or cancel the activation if necessary.

3. Check the default SD-Security settings under **Project specifications > SDN > SD-Security** and adjust them if necessary.



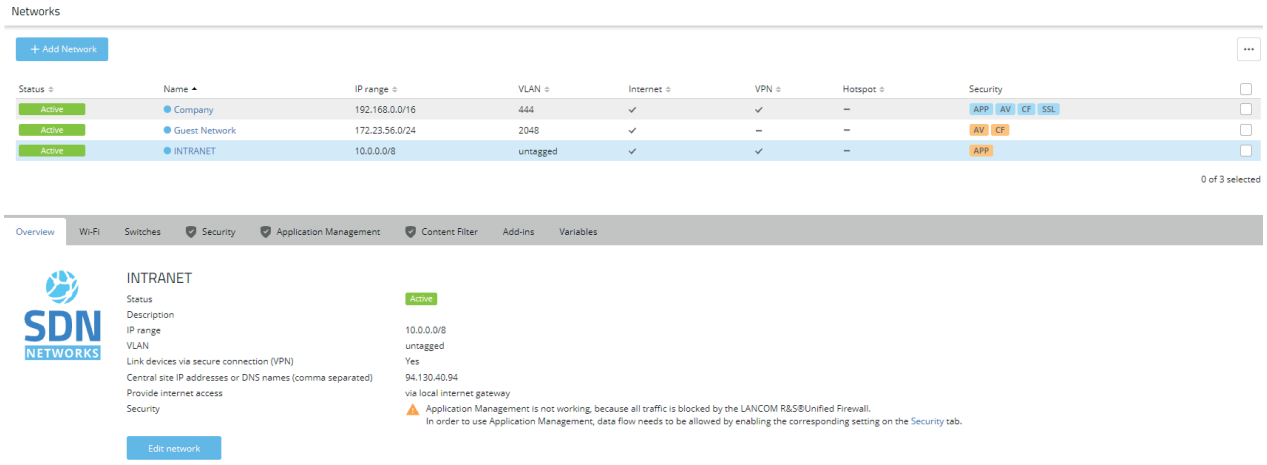
› If necessary, enable the use of the **Cloud Sandbox**.
The Cloud Sandbox extends the anti-virus protection and is only active on networks where the anti-virus protection is active. To protect against threats that are not yet known, the LANCOM R&S®Unified Firewall can upload suspicious files to a protected cloud. In this separate environment, they are safely and reliably tested using Machine Learning and Sandboxing.

If you enable the Cloud Sandbox, then the **Machine Learning features** will also be enabled.

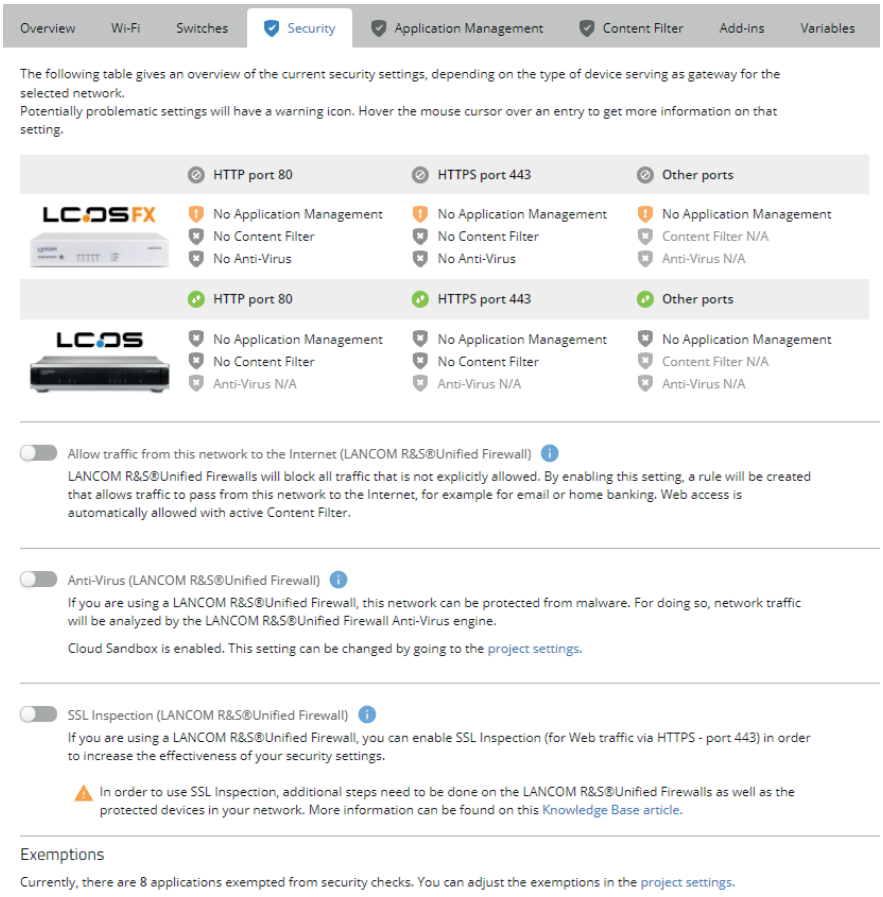
› Check the exception lists to see if a service still needs to be entered or deselected for your network.

4. In the **Networks** section, you now have additional settings available to enable more security features.

   Under the network definition — e.g. INTRANET — you will now find additional tabs:



› **Security** tab



i. In the overview you can see which security functions you have activated for which LANCOM product. A mouse hover effect over the icons provides you with further information.
ii. Allow traffic from this network to the Internet (LANCOM R&S®Unified Firewall)
This option allows full access to the Internet (Pass-All). Alternatively, you can perform a more detailed configuration via the web interface of the LANCOM R&S®Unified Firewall.
iii. Anti-Virus (LANCOM R&S®Unified Firewall)
Traffic between this network and the Internet can be routed through the anti-virus engine of the LANCOM R&S®Unified Firewalls to detect and block suspicious files before they enter your network.
In order to be able to check encrypted data traffic as well, SSL Inspection must also be activated and set up.
iv. SSL Inspection (LANCOM R&S®Unified Firewall)
If you have a LANCOM R&S®Unified Firewall, you can activate SSL Inspection to also control encrypted data traffic and thus increase the effectiveness of your security settings. This setting is available per network and can therefore be adjusted in the network settings.

UTM features such as Anti-Virus and Content Filter require SSL Inpection. If SSL Inspection is active in the LANCOM R&S®Unified Firewall, the LANCOM R&S®Unified Firewall redirects HTTPS connections to itself and acts as a proxy between the end device and the server. The end device must explicitly accept this by trusting the Proxy Certificate Authority of the LANCOM R&S®Unified Firewall.

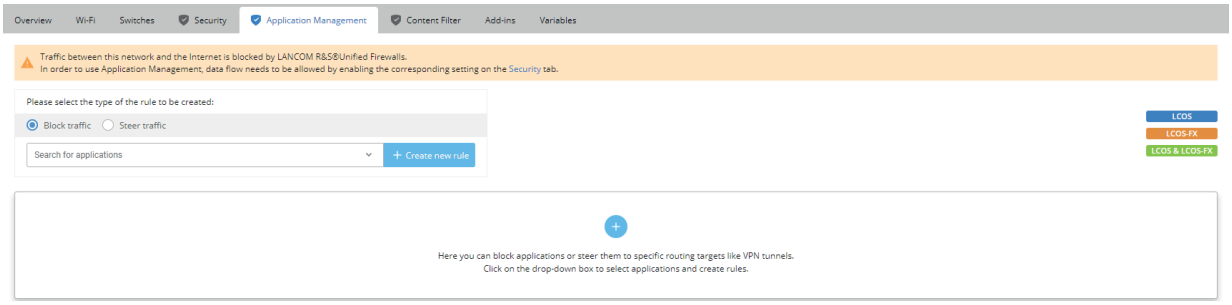
Necessary manual setup of certificates on the LANCOM R&S®Unified Firewalls during SSL inspection

If there are multiple LANCOM R&S®Unified Firewalls at multiple sites, there are two options:

a. CA per firewall: Each LANCOM R&S®Unified Firewall has an independent proxy certificate authority.
b. Company-wide CA: If an end device trusts a previously created and superordinate CA, it can be used at all sites without further effort.

Both cases are described in our Knowledge Base article, and LMC already takes care of some of the steps described there. However, there is still the installation of the certificates, which has to be done manually.

Application Management tab



We distinguish between three categories in application management:

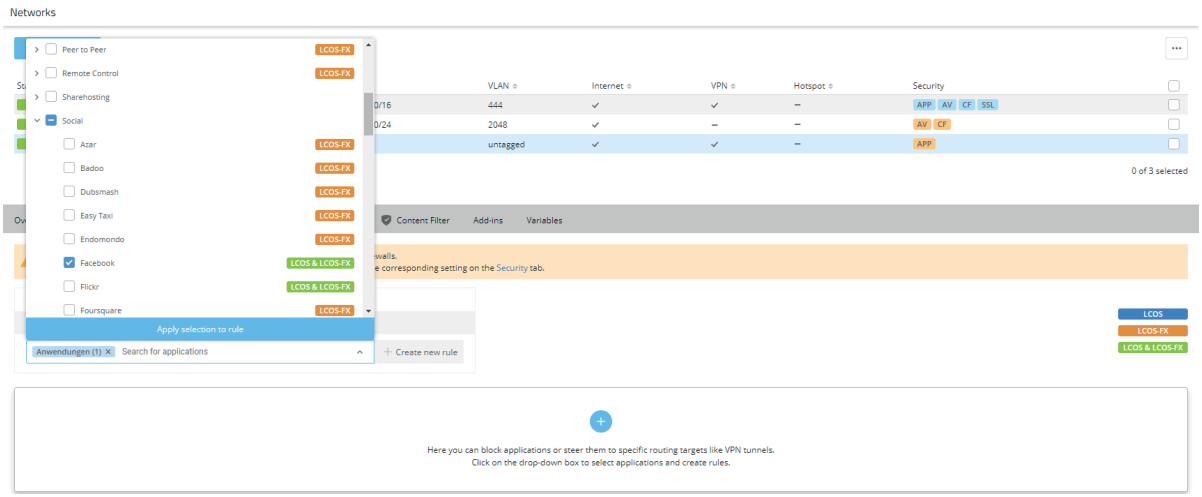
LCOS (Blue)	LCOS-based devices (routers) such as LANCOM 1926VA
LCOS FX (Orange)	LANCOM R&S®Unified Firewalls
LCOS & LCOS FX (Green)	LCOS-based devices (routers) and LANCOM R&S®Unified Firewalls

With this information you can check which service is detected by your device.

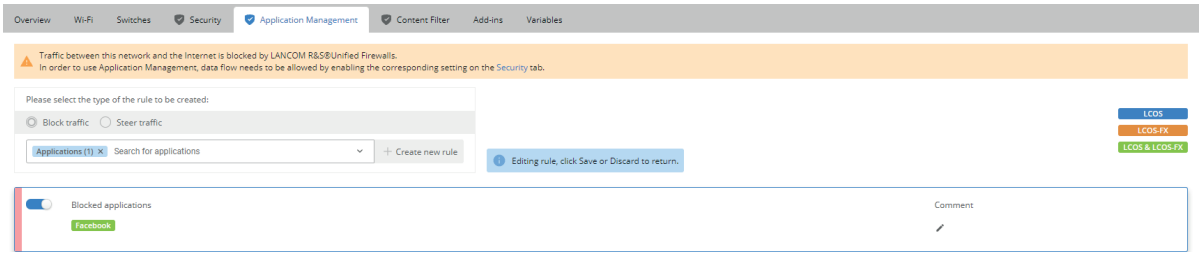
You can either block or steer the traffic:

i. Block traffic

You can block the traffic such as to “Facebook” very easily for a network: Select the **Block traffic** checkbox in the upper area of Application Management. Then click the **Create new rule** button and in the new dialog that appears you can select one or more services.



Apply your selection via the **Apply selection to rule** button. A created rule will be activated by default.



In this network, incoming and outgoing data traffic to the Internet is currently blocked by LANCOM R&S®Unified Firewalls. To use Application Management, you must first allow data traffic by setting the **Allow traffic from this network to the Internet (LANCOM R&S®Unified Firewall)** option on the **Security** tab.

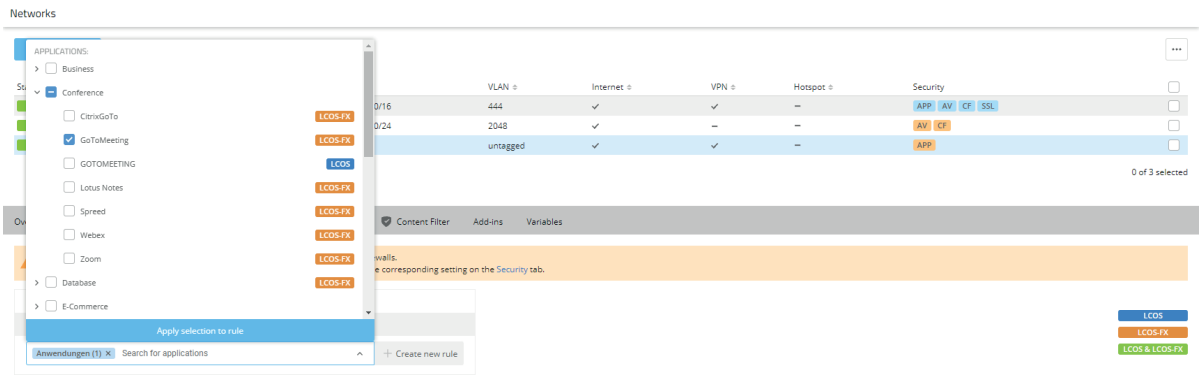
ii. Steer traffic

In the upper area of Application Management, select the **Steer traffic** checkbox.

Application redirection is supported only by LCOS-based devices at the time of writing. The feature will be provided for LCOS FX based firewalls until the end of 2021. Time-critical applications will be excluded from the SSL proxy on LCOS FX until then, but currently still forwarded without Local Internet Breakout.

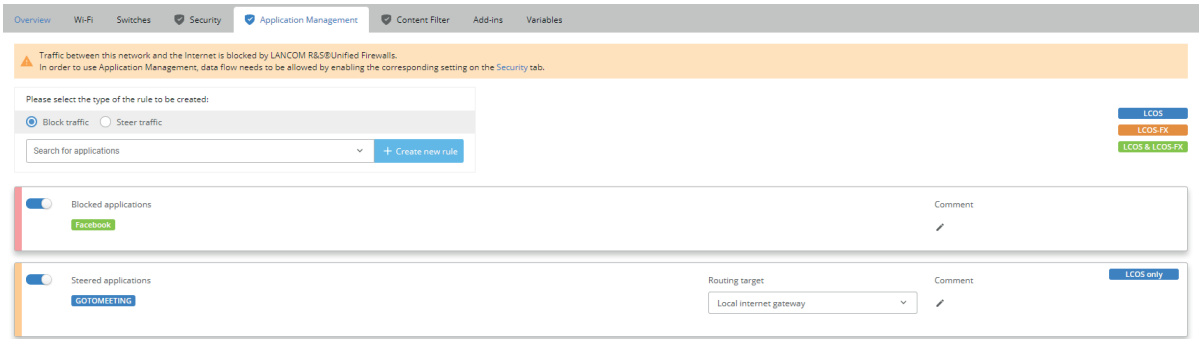
The LANCOM R&S®Unified Firewall can also redirect applications and/or protocols. However, you would have to set this manually via the web interface.

You can redirect the traffic such as to the conference service "GoToMeeting" very easily for a network, for that click the **Create new rule** button and in the new appeared dialog you can select one or more services.

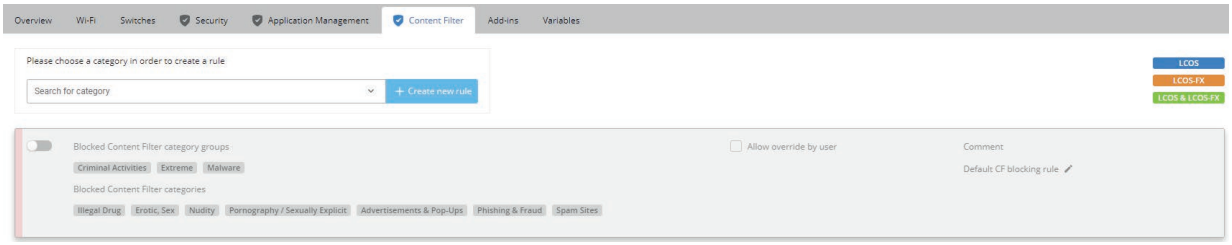


You need to decide how you want to redirect the traffic. You can do this in the **Routing target** drop-down menu.

For example, if you have selected for a network that all traffic is to be routed via the Central Site Gateway, you can have individual applications routed directly via an existing local Internet access (Local Internet Breakout).



› Tab **Content Filter**



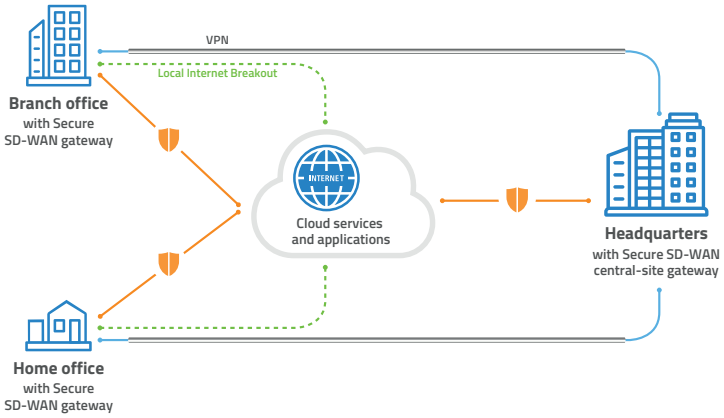
i. In this section, you can set the Content Filter rules for both the LANCOM R&S®Unified Firewalls and LCOS-based routers. As an example, we have provided you with a "Default CF blocking rule". In order for you to test our example rule, you would only need to activate it.

5. Once all settings are set correctly and both networks and devices are assigned to the site, you can roll out these configuration changes.

Exemplary application scenarios

Scenario 1: Decentralized security at all sites

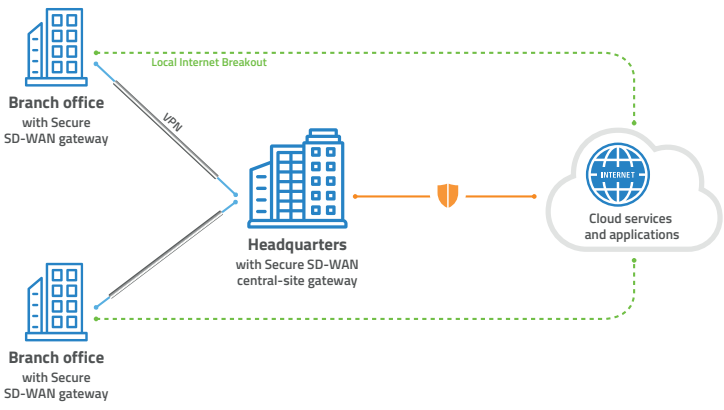
In this scenario, all branch offices are connected to the headquarters via SD-WAN/Auto-VPN for secure access to centrally hosted resources and services. A gateway with fully activated security functions is applied at each site, which means that the security requirements are defined individually for each site. In addition, latency for users is kept very low due to a Local Internet Breakout of trusted cloud-based applications. This scenario should cover most standard cases.



Recommendation: Deploy a local LANCOM R&S®Unified Firewall at each site. This allows you to achieve maximum performance through local Internet access while maintaining a high level of security through the firewall.

Scenario 2: Centralized security

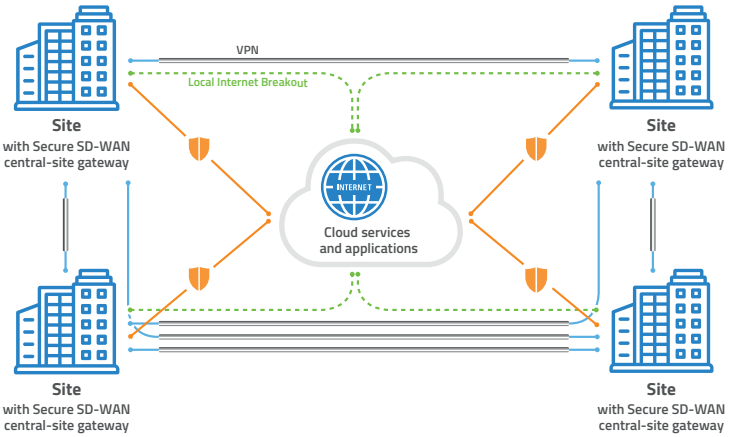
This scenario is ideal and cost-effective for smaller site networking scenarios. Here, just as before, all branch offices are connected to the headquarters via SD-WAN/Auto-VPN for secure access to centrally hosted resources and services. A high-performance gateway with fully activated security functions is applied in the headquarters, which defines the security requirements for all branch offices. In the branch offices, it is sufficient to apply smaller SD-WAN gateways without activated security functions, whereby a Local Internet Breakout for trusted cloud applications can reduce the traffic load in the headquarters.



This scenario is particularly suitable for cases in which local Internet access plays a subordinate role or is not required, for example, if machines are to be connected at the respective locations.

Scenario 3: Small networks – Equal sites without headquarters

In the case of company networks without a classic headquarters, all locations are completely interconnected with each other via Auto-VPN. A gateway with activated security functions is applied at all sites. The sites each have equal access to locally hosted services. Here, just as before, the security policies can be defined individually for each site, as can the Local Internet Breakout for trusted cloud applications.



LANCOM, LANCOM Systems, LCOS, LANcommunity and Hyper Integration are registered trademarks. All other names or descriptions used may be trademarks or registered trademarks of their owners. This document contains statements relating to future products and their attributes. LANCOM Systems reserves the right to change these without notice. No liability for technical errors and / or omissions. 10/2021