Avira Protection Cloud – Sandboxing and Machine Learning with the LANCOM R&S®Unified Firewalls

Malware and viruses are some of the biggest threats to network security. Virus signatures provide an effective defense against them. These signatures are rather like a unique digital identifier that is scanned to detect malware and files. Since new viruses are constantly being released or further developed, the signatures must also be continuously adapted. In order to maintain protection against malware and viruses even before the daily updates to the signatures arrive LANCOM cooperates with Avira to provide the Avira Protection Cloud. This Info Paper tells you more about the process of identifying malicious files with the Avira Protection Cloud.

Security against unknown threats

In order to protect against cyber attacks on previously unknown vulnerabilities (“zero-day exploits”), the LANCOM R&S®Unified Firewalls use machine learning and sandboxing. This test environment resides in a high-security cloud hosted in Germany, which uses third-generation machine learning to reliably analyze, scan, test, and block files as necessary.

Since LCOS FX 10.2, the operating system of the LANCOM R&S®Unified Firewalls works with the extended protection of the Avira Protection Cloud (APC), which addresses proactive queries about suspicious files. Every day, the constantly growing database of the Avira Protection Cloud is fed with thousands of new virus strains and is updated accordingly. It offers comprehensive protection against threats through heuristic detection and direct defense against potential threats.

How the Avira Protection Cloud works

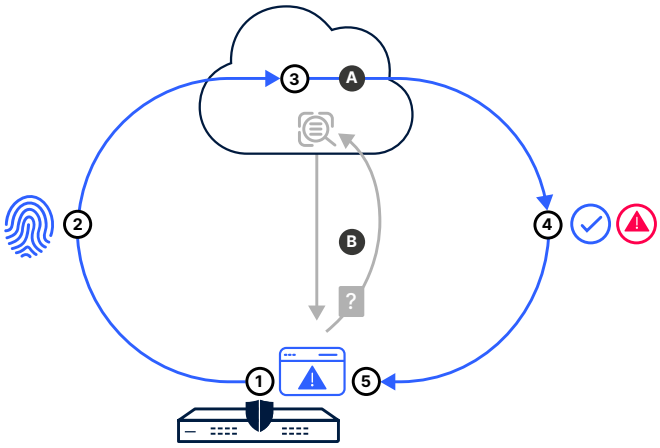

Figure 1:
Process for identifying malicious files in the Avira Protection Cloud

1. The local Avira engine initially scans new, unfamiliar files and checks them against the daily updated signatures of known viruses. The local check classifies the file as not suspicious, as infected based on its signature, or as “suspicious and unknown”.
2. If the file is classified as “suspicious and unknown”, a fingerprint of the file is extracted. This is done by creating a hash value to compress and anonymize the information.
3. The fingerprint is sent to the Avira Protection Cloud and compared there with all known fingerprints in the cloud. This closes the time gap between daily signature updates and new viruses. The check can again produce three possible results:
   a) The fingerprint belongs to a known, harmless file; it is a known piece of malware that has previously been analyzed by the Avira Protection Cloud;
   b) or the fingerprint is new to the Avira Protection Cloud. The complete file is then uploaded to the cloud, where it is analyzed in a sandbox in real time and “learned” as a new file.
4. To assess whether the fingerprint is dangerous or not, the Avira Protection Cloud refers to existing classifications or it uses machine-learning algorithms to reclassify the file.
5. The status of the fingerprint (hazardous or non-hazardous) is reported back to the LANCOM R&S®Unified Firewall, which manages the further actions.

About Avira

For over 30 years, the German company Avira (part of NortonLifeLock since 2020) has been a leader in the development of anti-malware technologies for companies of all sizes and for private users. The technologies are embedded in the security solutions from many of the world's leading network security companies.

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