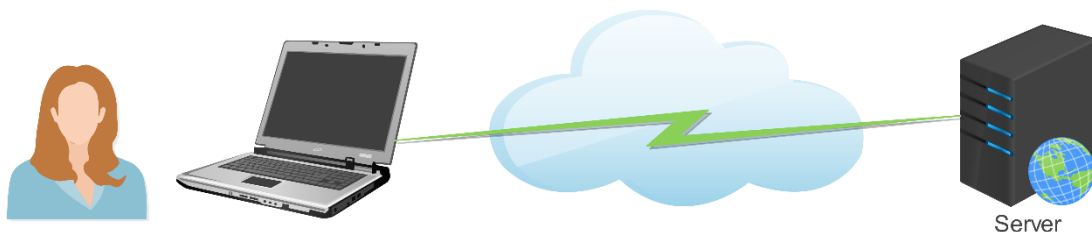


ApplicGate Man-in-the-Middle (MitM) Use Case

1 Initial situation

- The data sent and received by apps or browsers should be recorded.
- This function can be very helpful, for example, in program development.



2 Requirements

- All data must be logged.
- Encrypted connections (https) must be broken.
- No additional hardware should be necessary.
- Installation should be easy.

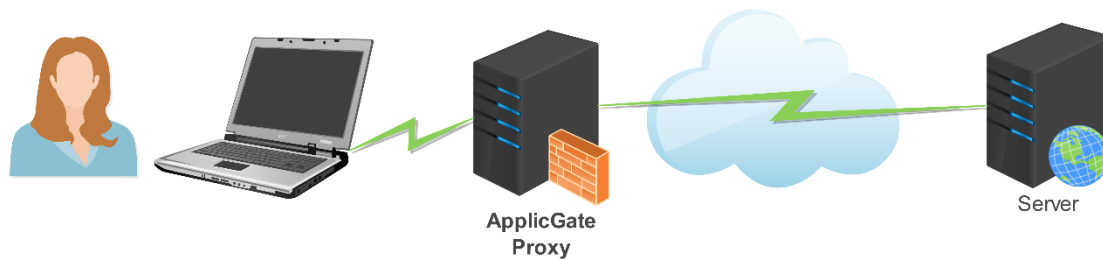
3 Solution by ApplicGate

ApplicGate is a software solution that runs on Windows and Linux and can be easily installed on existing systems.

Note:

Breaking encrypted connections is currently only supported under Windows.

3.1 Network schema



3.2 Fulfillment of requirements by ApplicGate

- **ApplicGate is configured as a web proxy** in WLAN/LAN.
- The devices communicate with the servers via this proxy.
- Encrypted connections (https) terminate at the proxy (data is decrypted). A new encrypted connection is established to the server (man-in-the-middle).
- The decrypted data is recorded.
- To break the https connection, the ApplicGate proxy automatically generates web server certificates with the appropriate names. These certificates are signed with a signing certificate. The signing certificate is generated using a PowerShell script, for example , and configured in ApplicGate.
- This signing certificate must be installed on the devices (Trusted Root Certification Authorities) so that the devices trust the certificates generated by ApplicGate.
- **Easy installation:**
The software is started with a mouse click and then configured via a web interface.
- **High availability :**
The ApplicGate Proxy can be backed up (hot stand-by).

4 Strengths of ApplicGate

- **Easy installation**
- **Flexible architecture :**
Can be installed on any Windows computer.

5 Table of Contents

1	Initial situation	1
2	Requirements.....	1
3	Solution by ApplicGate.....	1
3.1	Network schema.....	2
3.2	Fulfillment of requirements by ApplicGate	2
4	Strengths of ApplicGate	2
5	Table of Contents	3