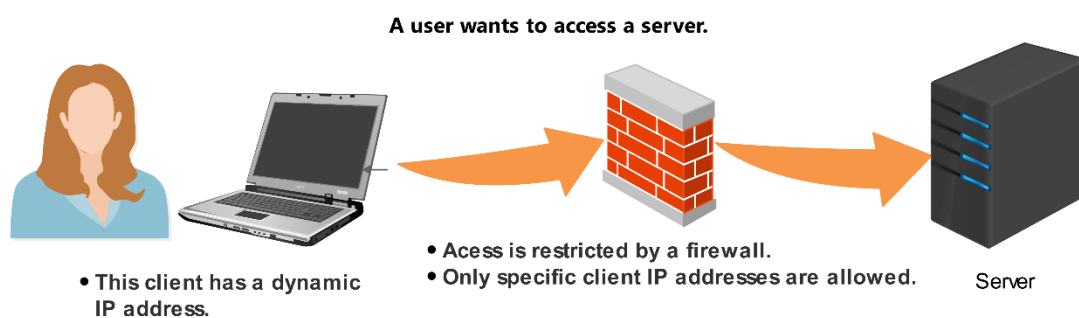


Access control for dynamic addresses

Use Case

1 Initial situation

- In a company, access to certain servers or applications on the server (e.g., databases) is secured by a firewall.
Access is only permitted for specific IP addresses.
- Many clients have a dynamic IP address, which therefore **cannot be configured in the firewall**.



- Note: The firewall in the image can also be a firewall integrated into the server.

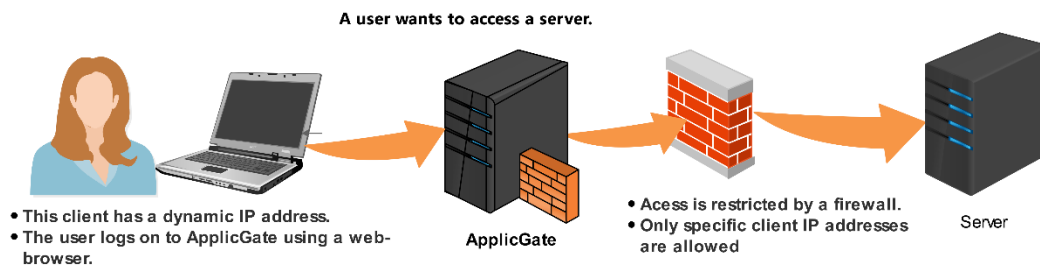
2 Requirements

- **Activating the firewall for dynamic client addresses.**
- **No changes** on the firewall or servers.
- **Logging of all access** for traceability and compliance.
- **Easy installation.**
- **High availability.**
- **Easy integration** into existing IT and security infrastructures:
Compatible with existing firewalls.

3 Solution by AppicGate

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

3.1 Network diagram



3.2 Fulfillment of requirements by AppicGate

- The user/client logs on to AppicGate using a web browser. This enables the routes configured for the user on AppicGate for the client's IP address. AppicGate communicates with the server using a fixed IP address.
- Various **strong authentication methods** are available for logon:
 - **One-Time-Password (OTP)** via email or SMS
 - **Time-based One-Time-Password (TOTP)** with Google or Microsoft **Authenticator**
 - **FIDO2** (with hardware token or passkey, e.g. Windows Hello)
 - **OAuth 2.0**
 - Software **certificates** or smart cards

Note:

With **OAuth 2.0**, an existing authentication (e.g. Microsoft Entra-ID, Google) can be adopted.

- If OTP, TOTP, or FIDO2 is used for authentication, the user must be created by an administrator in AppicGate. At a minimum, the email address must be provided. Optionally, times when the user can be active can be defined.
- When using certificates or OAuth 2.0, no user creation is necessary.
- TCP and UDP, IPv4 and IPv6 are supported to access the server.
- All **accesses are logged** on the AppicGate server.
- **Easy installation:**

AppicGate can be installed directly on the server or on any other computer. The preconfigured software is launched with a single click. The target address, web server certificate, and license are specified.
- AppicGate can be easily integrated into existing IT and security infrastructures and is compatible with existing firewalls.

4 Optional additional functions

- Time-dependent rerouting.

5 Strengths of ApplicGate

- **Development from practice** to easily upgrade existing installations.
- **Secure authentication**
- **Easy installation**
- **Flexible architecture:**
Can be installed directly on the server or any other computer (Linux or Windows).

6 Table of contents

1	Initial situation	1
2	Requirements.....	1
3	Solution by ApplicGate.....	2
3.1	Network diagram.....	2
3.2	Fulfillment of requirements by ApplicGate	2
4	Optional additional functions	3
5	Strengths of ApplicGate	3
6	Table of contents	3