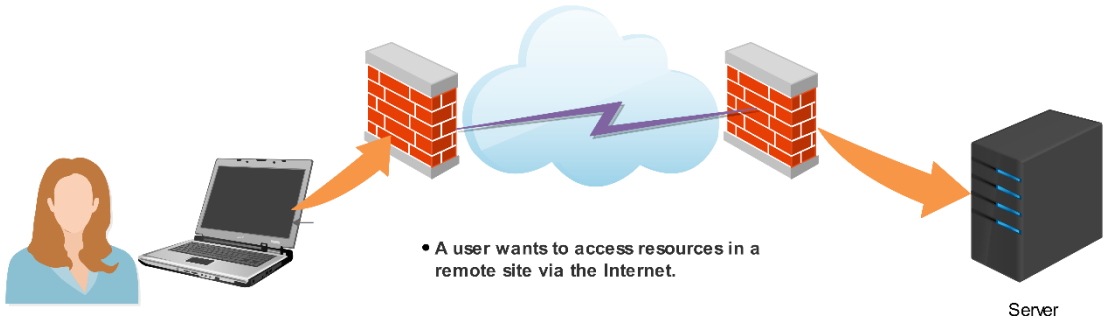
reinhold.leitner@applicgate.com
www.applicgate.com
2025-10-27

ApplicGate Site Connection Use Case

1 Initial situation

Two companies want to grant each other access to certain resources on their intranet under the following conditions:

- Both intranets are connected to the Internet.
- Internet access may not have a fixed IP address.
- Any address conflicts should be resolved.
- No additional hardware should be necessary.
- Installation should be easy.



Background:

A site -to -site VPN connection is complex to install and in many cases is not even necessary, especially if only selected resources are to be accessed.

Examples of resources to be accessed:

- Data via network drives (SMB) or Secure File Transfer Protocol (SFTP)
- Remote control of computers via SSH, RDP, VNC etc.
- Databases
- Applications
- Web server
- …

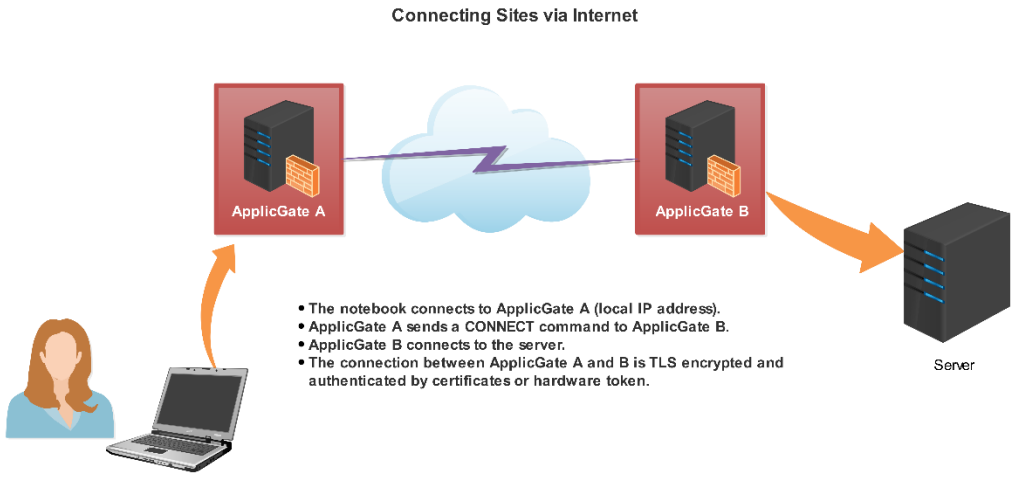
2 Requirements

- **Secure remote access** to other company's resources over the Internet.
- **Encryption** and **strong authentication** (multi-factor authentication, MFA)
- **Central management** of all access
- **Access control**: Each company should be able to see and control who accesses which resources at any time.
- **Logging of all accesses** for traceability and compliance.
- **No complex installation** at the customer's site.
- **High availability** – even at locations worldwide.
- **Easy integration** into existing IT and security infrastructures:
  No IP address conflicts, compatible with existing firewalls .
- **Support for various protocols** such as RDP, VNC, SSH, SFTP, SMB, HTTP(S), database access, etc.

3 Solution by ApplicGate

ApplicGate 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 ApplicGate

- **Secure remote access** to any target system via TCP or UDP, IPv4 and IPv6.
- If only temporary IP addresses are available on both sides, dynamic DNS is configured on one side. On the other side, there will only be **outgoing** connections via the internet, and ApplicGate will be addressed via dynamic DNS.

- **Encryption with TLS**
- Authentication between the ApplicGate systems is done using certificates or hardware tokens.
- Optionally, various **strong authentication types can** be configured for user access to ApplicGate:
  - Software **certificates** or smart cards,
  - **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**

  With **OAuth 2.0,** an existing authorization (e.g. Microsoft Entra-ID, Google) can be adopted→ Logon occurs automatically without user interaction.
- All access is **managed centrally on the ApplicGate server** .
- **Access control** :
  The IT administrator can enable and disable remote access. Automatic time control is configurable.
- All **accesses are logged** on the ApplicGate servers.
  Optionally, an email can be sent to specified addresses when a connection is established and /or terminated.
- **Easy installation** :
  The software is started with a mouse click and then configured via a web interface.
- **High availability** through various types of redundancy:
  The ApplicGate servers can be equipped with backup (hot stand-by).
- **The special routing architecture** enables **easy integration** into existing IT and security infrastructures. There are no IP address conflicts or complicated NAT rules in firewalls. Only an https connection to the internet is required. This makes the configuration compatible with existing firewalls.
- ApplicGate supports **all TCP protocols** and can **tunnel UDP** .
  For example, RDP, VNC, SSH, SFTP, SMB (network drives), HTTP(S), database access, etc.

4 Optional additional functions

- Automatic software update.

5 Strengths of ApplicGate

- **Secure authentication and granular rights structure**
- **Easy installation**

- **Control** :
  The IT administrator can actively grant/block access and see live who is connected.
- **Protocol diversity**
- **Flexible architecture** :
  Can be installed on any Linux or Windows machine.
  Redundancies can be configured.

6 Table of Contents