REMOTE ACCESS

WWW, DIRECT PORTS, ...

PROBLEM

Organisations increasingly need time limited remote access to network-enabled industrial devices or computer systems to facilitate efficient management, and control from virtually any location.

However, directly exposing these systems to the public internet introduces substantial security risks, making them susceptible to unauthorised access, cyberattacks, and data breaches.

Many of these systems were not originally designed with modern cybersecurity standards in mind and may lack support for secure protocols such as HTTPS. As a result, allowing unencrypted HTTP traffic significantly heightens the risk of interception and exploitation, compromising both operational integrity and sensitive data.

Addressing these challenges requires a secure, reliable, and easy-to-deploy solution that enables remote access without undermining the security posture of the organisation

CHALLENGE

How can an organisation establish highly secure, temporary connections to remote industrial devices or computer systems in a way that ensures data integrity and protection against cyber threats, while also avoiding the need for permanent exposure to the public internet?

Additionally, how can this be achieved in a cost-effective manner that reduces ongoing maintenance efforts and minimises the complexity of managing remote access infrastructure?

dbr

SOLUTION

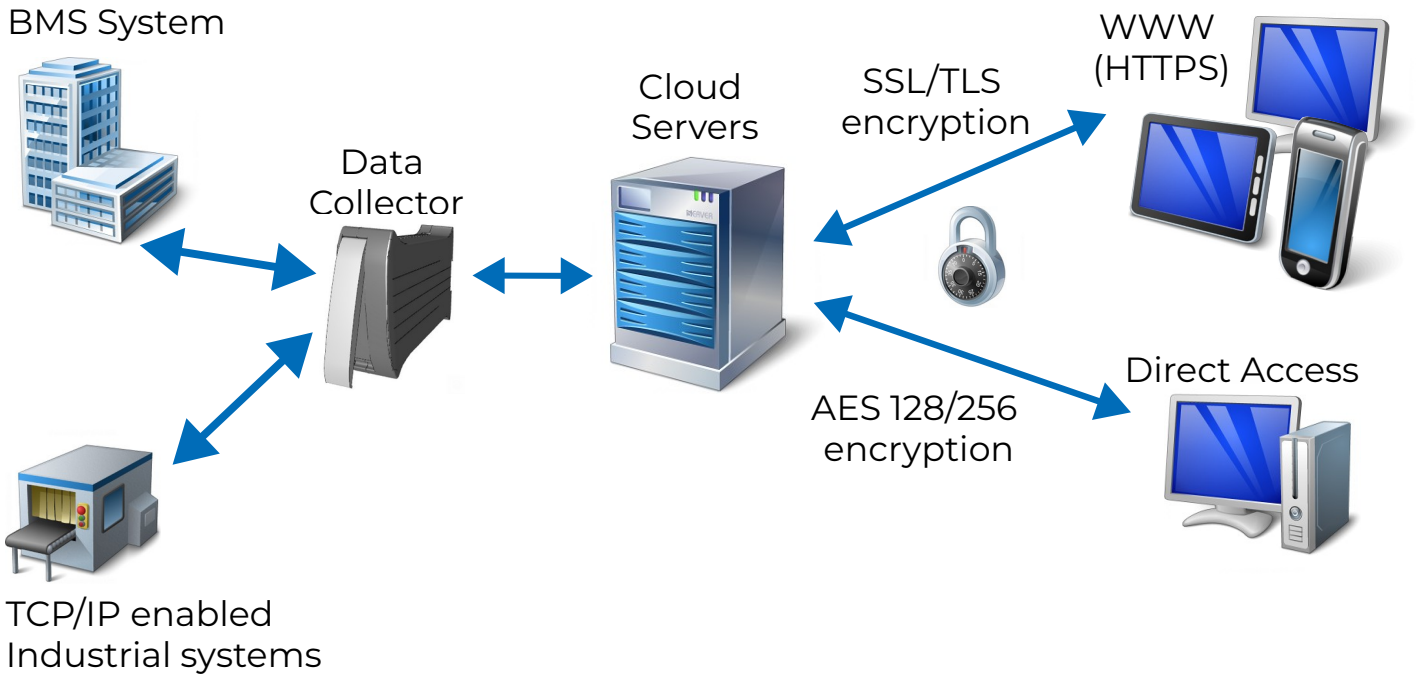
Our system serves the purpose of establishing a secure connection to a specific device's IP address and port. It accomplishes this by creating time limited encrypted tunnel that facilitates the transmission of traffic between the desired device and our public server.

We also offer the capability to monitor devices through direct port connections, such as service access. This functionality allows for service level access, enabling users to efficiently monitor and manage devices directly through their respective ports.

For HTTP connections, we go a step further by adding an SSL layer encryption on our server. This SSL encryption provides an additional layer of security, assuring the confidentiality and integrity of the communication.

Furthermore, to enhance security even more, we provide access via randomised URLs, adding an extra level of obscurity and reducing the risk of unauthorised access.

SCHEMATICS



CONTACT

mail@dbr.co.uk
+44 1268 442888