Enterprise-Grade
Data Security with VAULT™

In today's highly connected business landscape, organizations rely on secure, centralized control to manage intrusion and access systems across multiple locations. As cybersecurity threats continue to evolve, protecting sensitive data and maintaining network integrity is more critical than ever.

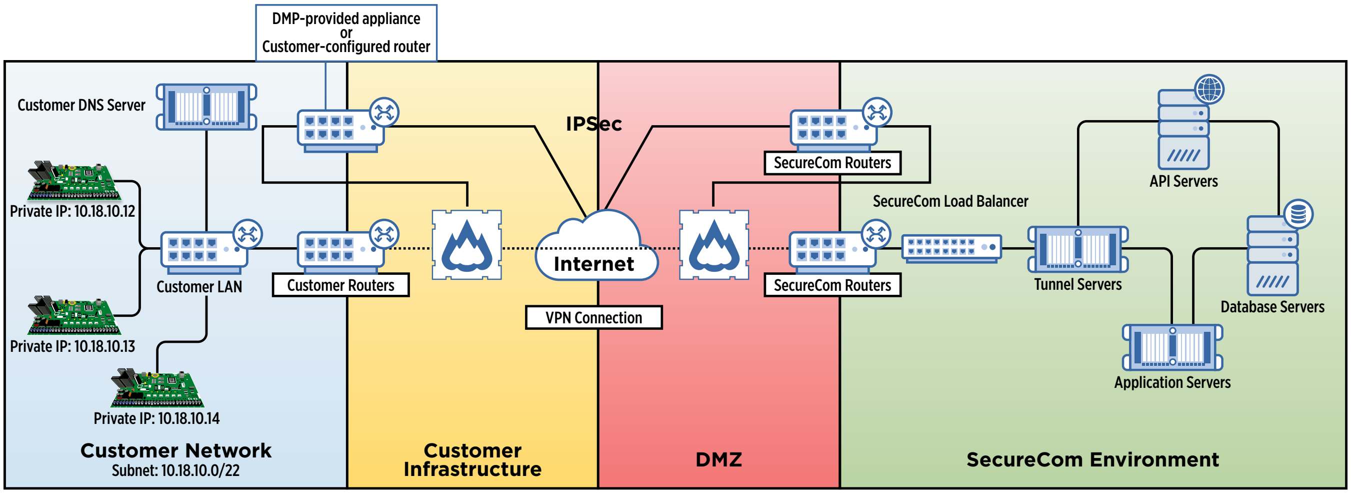
For enterprise customers requiring the highest level of data security, SecureCom™ offers Virtual Access Using Layered Tunneling (VAULT). This architecture is a dedicated Point-to-Point Virtual Private Network (VPN) built on IPSec (Internet Protocol Security) — a robust framework for securing IP communications through strong authentication and encryption.

This site-to-site VAULT establishes a fully encrypted tunnel between your corporate Local Area Network (LAN) and the SecureCom server infrastructure.

With VAULT in place:

- DMP security panels communicate directly and securely with SecureCom servers.
- The Domain Name System (DNS) is used to resolve server hostnames to IP addresses for efficient routing.
- No panel is ever exposed to the public internet, dramatically reducing risks from external threats.

Once a Transmission Control Protocol (TCP) session is established, the DMP panel maintains a persistent, secure connection with SecureCom servers. This allows for immediate responsiveness when accessed through the Virtual Keypad platform. The connection can also be terminated from the customer infrastructure if the need arises.



DEPLOYMENT SUPPORT

To simplify implementation, DMP provides enterprise customers with a preconfigured VAULT appliance, ensuring a streamlined and secure deployment process. For customers using their own firewall or router, DMP's IT Department can assist with the VAULT configuration, including setup of IPSec parameters, key exchange and routing policies.

SECURITY BENEFITS

With VAULT, your organization gains a trusted, hardened communication channel with the following security advantages:

- **Multi-Layered Encryption:** IPSec uses a combination of encryption protocols such as AES (Advanced Encryption Standard) and SHA (Secure Hash Algorithm) to ensure both confidentiality and integrity of data. These protocols operate at the network layer, securing all traffic regardless of the application in use.
- **Authentication and Key Exchange:** The VPN tunnel is secured using Internet Key Exchange (IKEv2) with either pre-shared keys or X.509 digital certificates to authenticate both endpoints. This ensures that only trusted networks can establish connections.
- **Data Integrity & Anti-Replay Protection:** IPSec includes integrity checks and sequence numbering to detect and block replay attacks or tampered packets in real time.
- **Tunnel Mode Encapsulation:** IPSec is configured in Tunnel Mode, meaning the original IP packets are fully encrypted and encapsulated within new headers. This isolates panel traffic from all external visibility and provides full encapsulation of payload and routing information.
- **Always-On Availability:** The persistent nature of VAULT ensures that panels remain in constant, encrypted contact with SecureCom servers — ready for real-time interaction via the Virtual Keypad platform.
- **Rapid Connection Termination:** In the event of a detected threat, breach, or policy violation, administrators can immediately terminate the VPN tunnel. This allows for swift isolation of affected systems, minimizing risk and containing potential damage.

This layered and rigorously engineered approach to security offers enterprise customers a comprehensive, end-to-end solution for protecting physical security systems and sensitive data.

The VAULT solution ensures that communication remains private, authenticated and protected — meeting the high standards demanded by modern enterprises.