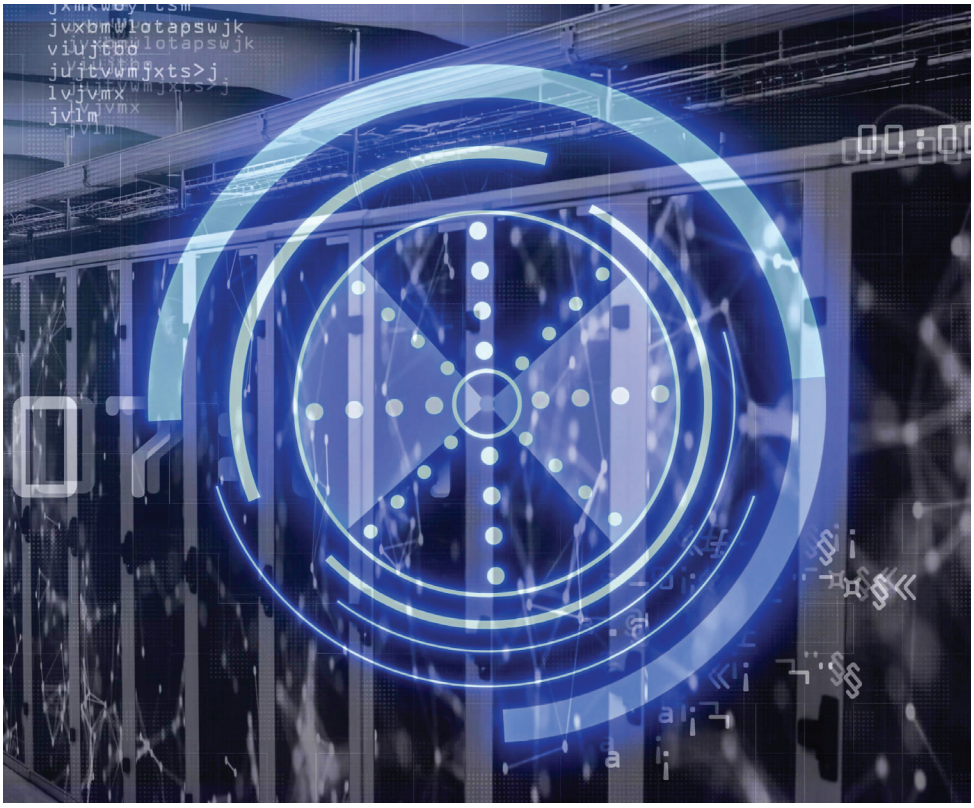
VAULT™ Virtual Access Using Layered Tunneling



Benefits

- Panels remain in constant, encrypted contact with SecureCom™ servers
- No panel is ever exposed to the public internet, dramatically reducing risks from external threats
- In the event of a detected threat, breach, or policy violation, administrators can immediately terminate the VPN tunnel
- Multi-layered encryption secures all traffic regardless of the application in use

Features

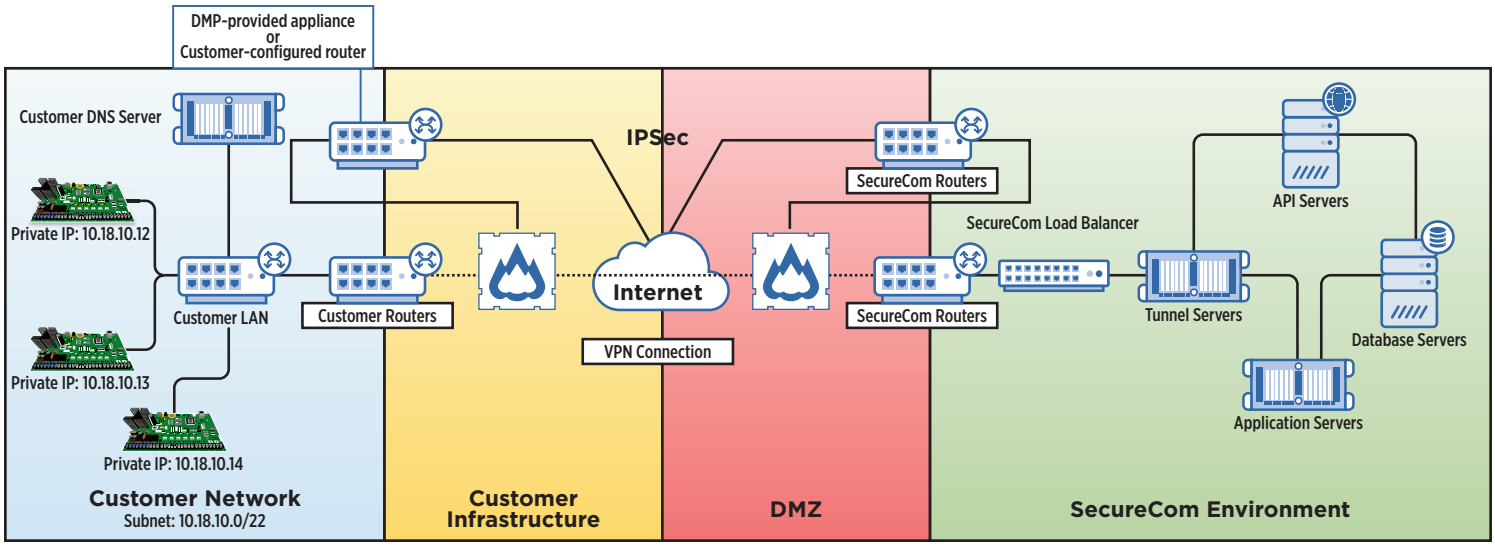
- Uses a combination of encryption protocols such as AES (Advanced Encryption Standard) and SHA (Secure Hash Algorithm)
- Secured using Internet Key Exchange (IKEv2) with either pre-shared keys or X.509 digital certificates to authenticate both endpoints
- Configured in Tunnel Mode to isolate panel traffic from all external visibility, providing full encapsulation of payload and routing information
- The Domain Name System (DNS) is used to resolve server hostnames to IP addresses for efficient routing
- Integrity checks and sequence numbering detect and block replay attacks or tampered packets in real time

VAULT Virtual Access Using Layered Tunneling

For enterprise customers requiring the highest level of data security, SecureCom offers VAULT (Virtual Access Using Layered Tunneling). 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.

VAULT Hardware is a pre-configured router device for streamlined deployment. Institutions may elect to use their own equipment and take advantage of **VAULT Configuration**, a service DMP provides, including setup of IPSec parameters, key exchange and routing policies.



DMP.com | 800-641-4282
2500 N. Partnership Blvd
Springfield, MO 65803

LT-3120 10/27/2025