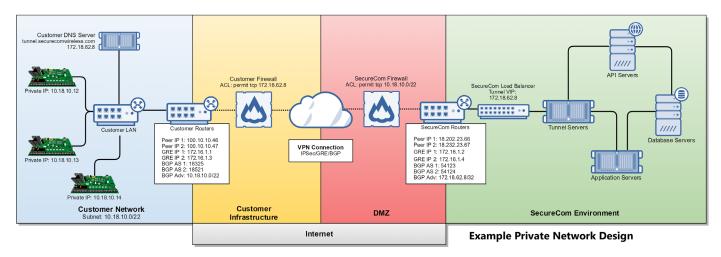# Customers Who Need the Highest Data Security

In today's digital world, businesses highly value the convenience of Virtual Keypad Access™ to manage access control and intrusion across multiple sites. Mobile security is paramount, and you need the assurance that your data is protected. We have a solution.

Some multi-site retailers and other enterprise-class customers want all panels talking to SecureCom™ servers in an encrypted environment. To meet those requests, we offer the option of using a dedicated Point-to-Point Virtual Private Network (VPN) that encrypts all communication from your corporate Local Area Network (LAN) directly to the SecureCom servers. At no time, therefore, will any control panel be open to the public Internet.

Example Private Network Design

The Most Secure Cloud-Based Communication Available

When choosing a network security solution, a site-to-site VPN is unparalleled for secure communication. The privacy of a VPN is due largely to the fact that all packet data sent across the Internet is encrypted and encapsulated before being transported. This fully encrypted connection is ideal for communications, including Virtual Keypad app access over EasyConnect™.

With the addition of a site-to-site VPN, you have secure private network access to the SecureCom Virtual Keypad platform. The DMP security panel will be able to directly communicate to the SecureCom servers using the Domain Name System (DNS) protocol, which translates domain names to IP addresses.

Once a TCP session is established, the DMP panel remains connected to the SecureCom servers. This ensures that the panel is available immediately on demand for app connections. The VPN connection is encrypted, and data from your panels are encrypted while being transported over the Internet via the VPN tunnel to SecureCom's servers.

Furthermore, the Virtual Keypad app connects to the SecureCom servers using industry-standard encryption, Transport Layer Security (TLS). TLS ensures that data being transferred between the Virtual Keypad app and the servers remains encrypted during transport. The SecureCom team enforces strong algorithms to encrypt data in transit, preventing hackers from reading it as it is sent over the app connection.