Critical Infrastructure

High-Assurance VPN Encryption Appliance
for Secure Communications with NA366

AXIOMTEK®

www.axiomtek.com

High-Assurance VPN Encryption for Secure Government Communications with NA366

For government and defense organizations, protecting sensitive information transmitted over public IP networks is mission-critical. Secure communication between headquarters, branch offices, and remote sites depends on effective encryption and reliable hardware.

A cybersecurity company specializing in high-assurance encryption selected Axiomtek's NA366 as the hardware platform for its VPN encryption appliance. Axiomtek customized the NA366 to meet the customer's requirements for government, defense, and critical infrastructure applications, tailoring its network interfaces and integrating an OLED display, keypad, and power button. The customized NA366 retained its compact, fanless, low-power design and provided the hardware foundation for the customer's encryption technology.

Challenges

Protecting sensitive communications between government offices and remote sites required a hardware platform that could support the customer's VPN encryption solution within strict installation constraints. Limited cabinet space and cooling capacity restricted hardware selection. A compact, low-power appliance was essential to fit the available space and limit heat generation, while a fanless design would help reduce cooling-related maintenance. Reliable network connectivity and stable hardware operation were equally important to maintain communications across sites.

The platform also had to support the customer's operating procedures through a customized OLED display, keypad, and power button for local interaction. Physical protection was required to help prevent unauthorized access or tampering. The customer also required burn-in testing of every unit before shipment to identify potential hardware issues and reduce the risk of field failures.

Key Requirements

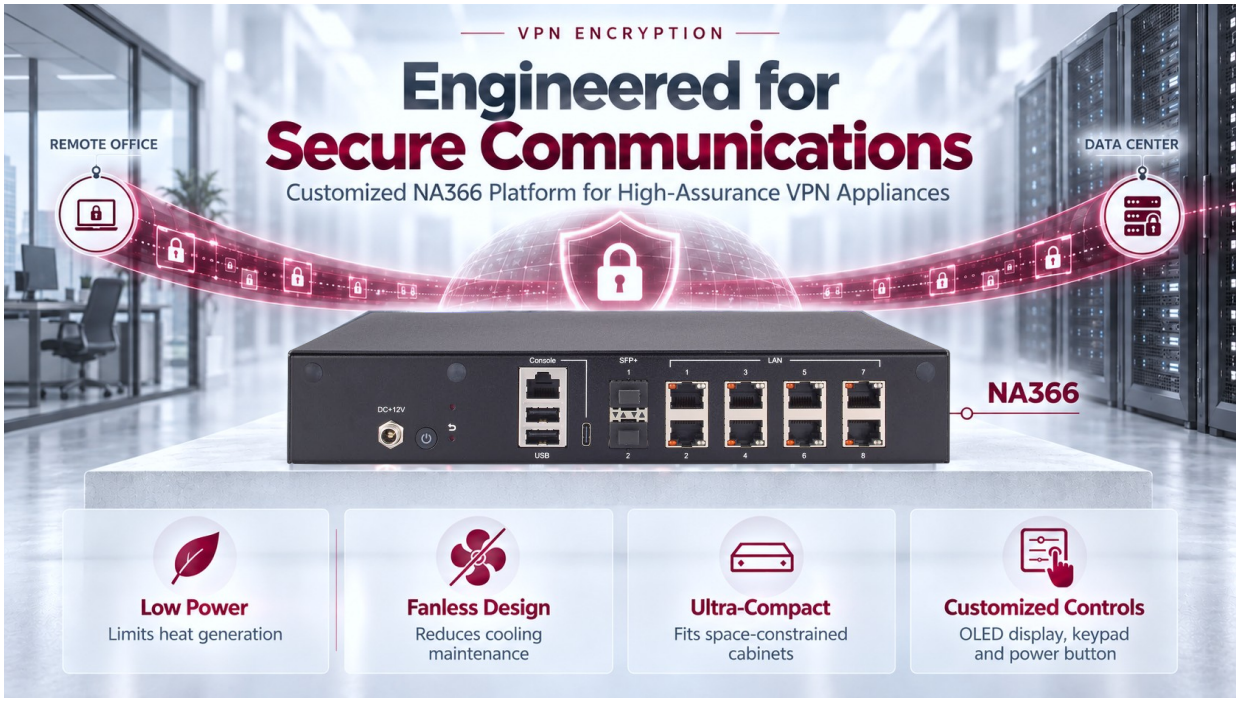
- Compact, rugged hardware for space-constrained cabinets
- Fanless, low-power design for installations with limited cooling capacity
- Reliable network connectivity for secure communications
- Customized OLED display and keypad
- Customized power button and operational controls
- Burn-in testing on every unit before shipment
- Stable long-term operation with minimal on-site maintenance

Solution

Customized NA366 Network Appliance

Axiomtek provided a customized NA366 network appliance as the hardware platform for the customer's VPN encryption solution. Its compact form factor enabled installation in space-constrained cabinets, while low power consumption limited heat generation in environments with restricted cooling capacity. The fanless design also helped reduce cooling-related maintenance, supporting long-term operation across distributed government sites. Each customized NA366 also underwent burn-in testing before shipment to help identify potential hardware issues and reduce the risk of field failures.

To meet the customer's operating requirements, Axiomtek tailored the NA366's OLED display, keypad, and power button, providing a local interface suited to the customer's procedures. These hardware modifications allowed the customer to integrate its encryption technology into a platform adapted to both the installation environment and day-to-day operation. The customized NA366 supplied the computing and network hardware, while the customer's VPN solution performed the encryption needed to protect sensitive communications between sites.



Application

Encrypted Connectivity Across Government Sites

The application connects government headquarters or a central office with branch offices and remote government sites through VPN encryption appliances based on the customized NA366. Installed at both ends of each connection, the appliances run the customer's VPN solution to establish an encrypted tunnel over the public IP network. This tunnel protects sensitive and classified information in transit between locations, enabling secure communication across geographically distributed government networks.

At headquarters, application servers, data servers, and network management systems form the central network that supports operations across connected sites. Workstations and local servers at branch offices access these resources through their local VPN appliance, with traffic passing through the encrypted tunnel to the central office. This arrangement allows authorized personnel to exchange information and use centrally hosted applications while protecting communications as they travel over the public network.

System Configuration

Customized NA366

- Two GbE RJ-45 ports with Intel® I210-AT controllers
- Four GbE SFP ports with an Intel® I350-AM4 controller
- One customized power button
- Customized OLED display and keypad
- Two USB 2.0 ports
- One RJ-type console port
- Three LED indicators for power, storage, and GPO status

Why Axiomtek

Axiomtek combined flexible hardware customization, compact fanless design, and reliable network connectivity to deliver a platform tailored to the customer's secure VPN application. Customized network interfaces, OLED display, keypad, and operational controls simplified integration with the customer's encryption technology, while burn-in testing helped support reliable long-term deployment across distributed sites.

Customer Testimonial

> **Axiomtek delivered the compact, reliable platform we needed to bring our secure VPN solution into the field. Smart card integration and customized controls addressed our specific operating requirements, while the fanless design reduced maintenance needs. This gave us a dependable hardware foundation for protecting sensitive and classified communications across government sites.**
>
> — Senior System Engineer

About

Axiomtek Co., Ltd.

Axiomtek is a global provider of industrial-grade embedded computing solutions. Our portfolio includes embedded boards, industrial motherboards, embedded systems, industrial PCs, and rugged platforms. Designed to meet real-world deployment requirements, these products emphasize reliability, integration flexibility, and long-term availability to support product continuity.

Our solutions are widely adopted in industrial automation, machine vision and inspection, transportation, energy and utilities, smart retail, healthcare, and edge AI applications. With flexible I/O and expansion options, scalable performance, and consistent platform roadmaps, we help customers simplify integration, reduce redesign effort, and accelerate deployment across diverse operating environments.