Forcepoint

FIPS 140-3 Compliance with Forcepoint NGFW

As cybersecurity threats become increasingly complex to detect and prevent, government and federal agencies require solutions that not only deliver robust security but also meet stringent regulatory and compliance standards. Forcepoint Next-Generation Firewall (NGFW) is designed to address these critical needs, including compliance with the Federal Information Processing Standard (FIPS) 140-3.

Why FIPS 140-3 Compliance Matters

→ FIPS 140-3 compliance is essential for federal agencies and contractors to protect national security.

→ It helps maintain the confidentiality, integrity, and availability of critical data.

→ The standard ensures that cryptographic functions are secure and minimizes unauthorized access or data breaches.

→ FIPS 140-3 compliance promotes trust and transparency in security systems.

→ It is crucial for handling sensitive government or defense-related data.

FIPS 140-3 Compliance in Forcepoint NGFW

→ Forcepoint NGFW solutions integrate FIPS 140-3 validated cryptographic modules into core firewall capabilities.

→ These modules ensure sensitive data is encrypted, stored, and transmitted securely, in line with FIPS 140-3 requirements.

→ Validated algorithms and key management protocols provide a high level of data protection both at rest and in transit.

→ Forcepoint NGFWs help government agencies, contractors, and regulated organizations maintain compliance with security standards.

Key elements of Forcepoint NGFW FIPS 140-3 compliance include:

→ Cryptographic Module Validation: Forcepoint NGFW integrates NIST-validated FIPS 140-3 cryptographic modules, ensuring firewall operations meet recognized security standards.

→ Secure Key Management: The NGFW solution supports strong key management, ensuring keys are securely generated, stored, and destroyed to maintain cryptographic integrity.

→ Data Encryption: Forcepoint NGFW uses FIPS-compliant encryption algorithms to secure communication and protect sensitive data from unauthorized access.

→ Secure Operation and Integrity: The NGFW solution implements security measures to protect cryptographic operations, preventing tampering and unauthorized access.

Forcepoint helps government agencies meet strict regulatory standards, protect sensitive information, and maintain national security by ensuring encryption, data integrity, and secure key management.

Learn more about **Forcepoint NGFW solutions,** and read more on **NIST FIPS 140-3**.