

Netilla Security Platform (NSP) FIPS Support

Meeting Rigorous U.S., Canadian and U.K. Security Standards



Government departments and federal agencies that manage access to highly sensitive applications need 100% confidence that their private data remains totally secure. The AEP Netilla Security Platform (NSP) with Federal Information Processing Standards (FIPS) support is designed to provide secure remote access to highly confidential data to meet the most stringent U.S., Canadian and U.K. security standards.

Secure Your Infrastructure with FIPS Protection

The FIPS-certified AEP Netilla Security Platform (NSP), a Secure Sockets Layer (SSL) VPN appliance, enables secure, Web-based, FIPS-compliant remote application access at the rigorous security levels that government networks require. With the FIPS protection, employees and trusted partners can quickly and securely reach key applications and sensitive data while meeting the most stringent public sector security requirements in use today.

NSP FIPS Security Features

- Incorporates AEP's FIPS 140-1 Certified Hardware Security Module (HSM)
- Key storage, signature and key generation in a factory installed hardware option
- Tamper protection
- Integrated Omniport interface for backup, configuration, and enable/disable functionality
- Application Layer Proxy protects your servers from direct access
- Robust client integrity options: Secure Desktop, Cache Cleaner, Host Integrity and Adaptive Policies
- Session inactivity timeouts and periodic user re-authentication
- PKI with client-side certificates with revocation support
- Stateful Packet Inspection Firewall built-in

Meeting FIPS 140-1 Compliance

FIPS 140-1 describes the security requirements for cryptographic products used by the U.S., Canadian, and other governments. Vendors must meet these requirements to sell cryptography products to public sector organizations, and increasingly to areas of the private sector such as financial services and healthcare.

The Netilla Security Platform's HSM is certified to FIPS 140-1 Level 3, the highest level of any similar product in the marketplace. AEP Networks is the only company to own its FIPS-compliant Hardware Security Module technology with FIPS certification.

NSP FIPS-Certified Cryptographic Module

The FIPS-certified NSP, a factory-installed solution, leverages AEP Network's revolutionary ACCE (Advanced Configurable Crypto Environment) technology. ACCE is the next generation, flexible cryptographic platform that provides the highest levels of assurance: FIPS 140-1.

- All AEP Networks' FIPS products incorporate ACCE technology—the most advanced crypto hardware environment available
- AEP Networks leading hardware and crypto engineers have over 100 years of combined experience to bring new levels of security, speed and manageability to our range of hardware security devices
- ACCE's low power, highly integrated design leads to increased reliability and savings in overall lifecycle costs

Meeting U.K. CESG Requirements

The FIPS 140-1 standard is recognized by the British government's Communications-Electronics Security Group (CESG) as meeting its "private"-level data security criteria. CESG is the British government's national technical authority for information assurance.

AEP Networks – The FIPS Specialist

AEP has vast experience developing FIPS-level security solutions in the AEP SmartGate, Keyper hardware cryptographic modules and Net range of products. For more information, please contact AEP Networks.

Corporate Headquarters	Government Solutions
AEP Networks 347 Elizabeth Ave., Suite 100 Somerset NJ 08873	AEP Networks 40 West Gude Drive, Suite 200 Rockville, MD 20850
Toll-Free: 1-877-638-4552 Tel: +1 732-652-5200	Toll-Free: 1-800-495-8663 Tel: +1 240-399-1200
Europe	Asia-Pacific
AEP Networks Focus 31, West Wing, Cleveland Road Hemel Hempstead Herts HP2 7BW U.K.	AEP Networks 2107 Tower 2 Lippo Centre 89 Queensway Hong Kong
Tel: +44 1442 458 600	Tel: +852 2845 1118
Japan	
JOYO Bldg 6-22-6 Shimbashi Minato-ku Tokyo 105-0004 Japan	
Tel: 81-3-3437-5663	



