随着网络攻击和数据泄露事件日益频发，数据加密已经成为网络安全防护的核心组成部分。数据加密通过将敏感信息转换成无法读取的加密格式，保障信息在存储和传输过程中不会被未经授权的访问者获取。无论是企业的客户数据、财务信息还是公司机密，数据加密都能有效降低外部威胁的影响，确保数据的机密性、完整性和可用性。

为了进一步加强数据安全，硬件级别的加密技术逐渐成为关键解决方案。**TPM 2.0**（受信平台模块 2.0）是一种硬件安全技术，它通过加密密钥的安全存储和硬件保护，为操作系统、应用程序以及数据提供物理层面的安全保障。TPM 2.0 不仅能为设备提供启动时的安全性，防止恶意软件攻击，还能在加密操作中为数据保护提供额外的防护层。

**AWS Nitro TPM 2.0** 是 Amazon Web Services 推出的硬件安全模块，旨在为云服务中的虚拟机提供可信的硬件级别的安全保护。与传统的基于软件的加密技术相比，Nitro TPM 2.0 提供了更高的安全性，因为它在硬件层面防止了密钥泄露的风险。这使得 Nitro TPM 2.0 在支持数据加密、密钥管理和防止数据篡改方面尤为重要，尤其适用于需要高安全性的应用场景，如金融服务、医疗行业和政府机构等。

**Nitro TPM 2.0 的关键需求包括：**

1. **硬件安全**：通过硬件加密与密钥存储，确保数据在系统崩溃或被物理攻击时依然安全。
2. **增强的启动保护**：提供 UEFI 启动保护，防止恶意代码的注入和未授权的系统更改。
3. **合规性支持**：满足高标准的安全合规要求，如 GDPR、HIPAA 等。
4. **加密性能**：提供强大的加密计算能力，支持高效的数据加密和解密操作。

随着对数据安全性需求的不断提高，Nitro TPM 2.0 作为一种先进的安全解决方案，正逐渐成为许多企业和组织在云环境中确保数据安全、提升合规性的首选技术。

FortiGate是集下一代防火墙、高性能SSL/IPSec VPN网关、SD-WAN CPE于一身的新一代防火墙产品。Gartner企业防火墙和UTM魔力象限双料领导者，第三方评测实验室NSS Labs连续六次下一代防火墙小组评比获"推荐级"。具有性能高，安全效果好，功能丰富等特点。是用户在本地和云端进行安全组网、安全隔离、流量检查、行为监测的必备武器。

FortiGate-VM V7.6.1以及后续的版本支持 AWS Nitro 可信平台模块（NitroTPM）2.0 规范。NitroTPM 是 AWS Nitro 系统提供的符合 TPM 2.0 规范的虚拟设备。它能安全地存储用于验证实例的密码、证书或加密密钥等人工制品。NitroTPM 可以生成密钥，并将其用于散列、签名、加密和解密等加密功能。

启用TPM2.0加密优势保障Fortigate 配置，即使配置丢失也无法通过配置恢复的方式导出配置，复现用户使用场景。通过硬件加密与密钥存储，确保数据在系统崩溃或被物理攻击时依然安全。此外提供 UEFI 启动保护，防止恶意代码的注入和未授权的系统更改，满足高标准的安全合规要求。

如果需要TPM2.0镜像部署支持，请联系Fortinet 专业人员进行对接支持，联系方式+86 4006005255。

部署好后，验证fortigate实例 是否支持AWS Nitro TPM 2.0 ，并进行功能自检测试

A computer screen shot of a computer

AI-generated content may be incorrect.

A screenshot of a computer program

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

配置TPM加密，并产生随机密钥信息

A screen shot of a computer code

AI-generated content may be incorrect.

恢复出厂设置后，模拟配置被盗取在其他设备上尝试恢复配置，无法恢复配置提示密钥不匹配，验证TPM加密机制。

A black screen with white text

AI-generated content may be incorrect.

A black screen with text on it

AI-generated content may be incorrect.

客户常用使用场景：

TPM 2.0（可信平台模块 2.0）是一种硬件级安全芯片技术，主要用于增强设备和数据的安全性。它通过提供物理隔离的加密密钥存储、硬件级加密运算和安全认证等功能，满足多种客户和场景对安全性的高要求。以下是其适用的主要客户类型和典型场景：

1. **企业用户**
   * **数据敏感行业**：金融、医疗、法律等行业客户，需保护客户隐私、交易数据或机密文件。
   * **IT资产管理**：企业需对设备进行身份认证和完整性验证，防止未经授权的设备接入内网。
2. **物联网（IoT）设备厂商**
   * 智能家居、工业物联网等设备需通过TPM 2.0保障固件安全、设备身份认证和数据传输加密。
3. **合规性场景**
   * 满足行业法规要求（如GDPR、HIPAA、PCI-DSS），避免因数据泄露导致的合规风险。

Reference: <https://aws.amazon.com/blogs/aws/amazon-ec2-now-supports-nitrotpm-and-uefi-secure-boot/>

https://docs.fortinet.com/document/fortigate/7.6.0/new-features/329311/aws-nitrotpm-support-7-6-1