Next-Generation Encryption for Secure Connectivity at a Glance

In today's fast-changing world, data security is a top priority for government, utilities, public safety, and business enterprises. The number of cyber attacks targeting US organizations has doubled over the past three years, with more than 100 successful attacks per week and average losses for business of nearly $9 million per attack, according to a recent Ponemon Institute study. To help protect data in this rapidly evolving threat environment, Cisco's Next-Generation Encryption (NGE) technologies are now included in a wide portfolio of networking products. Cisco® NGE:

- Supports a new range of algorithms to secure data traffic against the next generation of attackers
- Securely connects remote users to each other and to the network
- Provides secure management capabilities and wireless functions
- Quickly adds new sites or users, without impacting existing infrastructure
- Improves productivity by extending corporate networks, applications, tools

The Constantly Evolving Data Security Threat

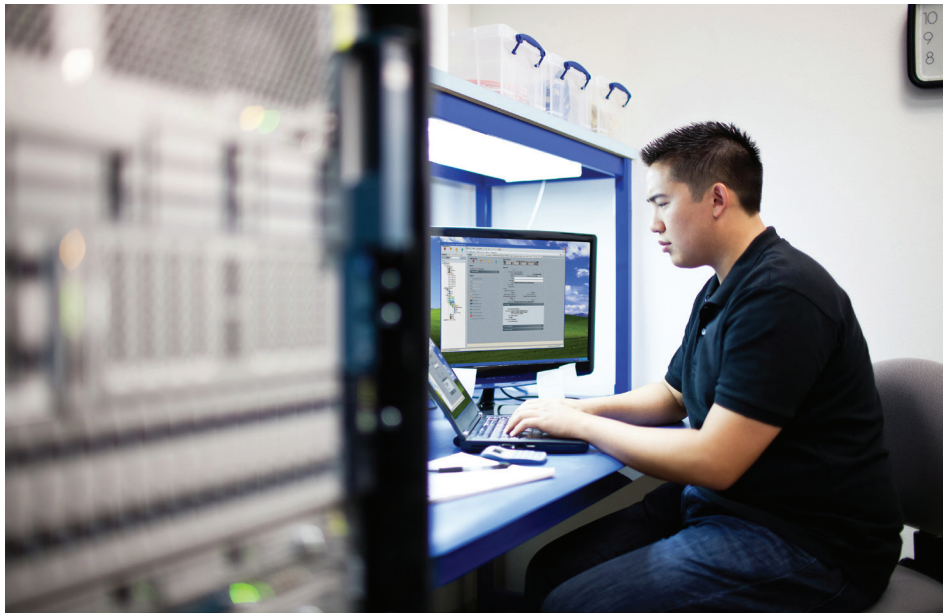
Threats to your sensitive data can literally evolve within days or even hours, as persistent, well-funded attackers continuously develop new ways to penetrate encrypted systems. Steady advances in computing and in the science of cryptanalysis have made it necessary to adopt newer, stronger algorithms and larger key sizes. However, some older algorithms and key sizes no longer provide adequate protection from modern threats, and even today's 128-bit systems are increasingly vulnerable to attack. These challenges are driving a move to higher cryptographic strengths such as Cisco NGE.

The Cisco NGE Solution

Cisco NGE leads the industry in advanced encryption, providing support for an extended family of U.S. and international standards. It is currently available on most Cisco virtual private network products and architectures, and is progressively being added to all Cisco technologies. It comprises globally created, globally reviewed, and publicly available algorithms–the result of more than 30 years of global advances and evolution in cryptography. Cisco NGE continues to support older algorithms to ensure backward compatibility and interoperability, while upgrading all cryptography mechanisms to today's standards and laying the groundwork for future security and scalability requirements.

Features include:

- Compatibility with international government standards, including Federal Information Processing Standards 140 Series (FIPS-140) (US/Canada), Health Insurance Portability and Accountability Act (HIPPA), Payment Card Industry Data Security Standard (PCI DSS); and standards in NATO countries, Germany, the United Kingdom, and Australia
- Upgraded algorithms, key sizes, protocols, and a complete algorithm suite in which each component provides a consistently high level of security
- Ability to effectively scale to meet high throughput and large numbers of connections
- Ability to scale down to meet the security needs of low-power devices while being efficient in battery use



The Power of Network-Based Encryption

Today's encryption solutions are often application-based, meaning that each application must support its own strong cryptography. Not surprisingly, this requires organizations to incur per-application operating and compliance costs. Applications may also suffer from lower performance; this is especially notable in today's rapidly expanding mobile environments. Cisco's solution is to encrypt, not each application, but the network itself. In a single powerful deployment, Cisco NGE protects applications, devices, and the data travelling over the network while centralizing and lowering IT costs, simplifying provisioning and updates, and achieving regulatory compliance. Network-based encryption is the most secure option for protecting data being transported over any network.

Cisco Encrypted Virtual Private Networks

Cisco's encrypted Virtual Private Network (VPN) solutions offer data security within private networks that are extended across public networks such as the Internet. Appearing to the user as private network links, VPNs actually create a highly secured wide area network (WAN) through the use of dedicated connections and encryption.

Site-to-Site VPNs

Cisco's Site-to-Site Encrypted VPNs provide reliable, high-quality transport of complex, mission-critical traffic over an Internet-based WAN infrastructure to branches, home offices, and business sites. From any location with an Internet connection, personnel may exchange highly encrypted data over an integrated network that features support for Quality of Service (QoS) and multicast. Networks may be customized using Cisco's advanced network intelligence and routing, while organizations take advantage of simplified provisioning and reduced management costs.

Remote Access VPNs

Cisco Remote Access Encrypted VPNs extend almost any data, voice, or video application to remote desktops and devices, supporting personnel who require NGE-level encryption, especially in mobile networks. Enterprise traffic is encrypted with NGE as it moves to and from hostile networks, providing highly secure, customizable remote access to anyone, anytime, anywhere. These solutions support a wide range of connectivity options, endpoints, and platforms while providing full encryption.

NGE is also embedded within special-purpose VPNs such as:

- Group Encrypted Transport VPNs (GET VPNs) for large-scale video and voice support
- Dynamic Multipoint VPNs (DMVPNs) for centralized management of mobile environments

Why Cisco NGE?

An industry leader in cryptography and security, Cisco NGE offers significant benefits across today's vital industries and national infrastructures. NGE is:

- Efficient at high security levels
- Increasing security while improving scalability to high speeds
- Upgrading the entire crypto suite
- Included in many other standards, including IPSec, TLS, MACSec
- Helping meet business and regulatory requirements for a variety of industries

Next Steps

Contact your Cisco account team to discuss how we can help secure your data using the next generation of cryptography.

C45-728370-01 4/14