White Paper

Meeting Today's Data Security Requirements with Cisco Next-Generation Encryption

Today's Encryption Environments

The number of cyber attacks targeting US organizational data has doubled over the past three years. Today's firms experience more than 100 successful attacks per week and average losses of nearly $9 million per attack, according to a recent study by the Ponemon Institute. Still worse are the results of government data breaches, with the potential for disruption or sabotage of public, utility, safety, and financial services. As the encryption algorithms protecting such data continues to age, these systems are becoming increasingly easy to penetrate, especially with mobile devices and centralized cloud services providing new points of access for attacking or stealing critical data.

Organizations are well aware of these problems, and over the past few years, data encryption has increasingly shifted from simple data breach remediation to becoming a key strategic business issue. Ponemon Institute studies demonstrate that companies and government agencies are increasingly working toward establishing management strategies that help to assure secure and operationally efficient encrypted systems.

A significant percentage of investment is therefore focused on achieving compliance with privacy or data security initiatives or regulation. Financial services, healthcare, retail, and public safety organizations are all looking for new ways to encrypt their environments, assure information security over managed carrier services, and secure data in the cloud and other shared infrastructures. Advanced technologies such as Cisco® Next-Generation Encryption (NGE) provide organizations with the tools they need to defend and maintain the security of information traffic.

The Evolving Data Security Threat

Cryptography is by no means static. Threats to sensitive data can literally evolve within days or even hours, as persistent, well-funded attackers continuously develop new ways to penetrate supposedly secure systems. Steady advances in computing and in the science of cryptanalysis have made it necessary to adopt newer, stronger algorithms and larger key sizes. Older algorithms and key sizes no longer provide adequate protection from modern threats. Currently effective encryption systems will become progressively less so. Over the next generation, new, stronger encryption technologies are needed to continue to secure data for the future.

Cisco 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. Relying on a single architectural foundation provides encryption support for:

- All applications, both current and future
- Any device, including mobile, legacy, and industry-specific devices
- All traffic, including multicast, control data, and messaging

The Cisco network enabled with NGE transitions readily to more advanced encryption capabilities, as opposed to having to upgrade each and every application. Once deployed, it supports regular provisioning and updates (including security patches) for better regulatory compliance. Centralized expert management also lowers maintenance costs compared to the price of maintaining many separate applications. As well, a single, consistent approach to network security helps to keep the entire system more secure, instead of relying on a variety of individual approaches from different application specialists. By providing a permanent foundation for ongoing data security, network-based encryption is the safest way to protect data in transit over the network, and enables new best practices in critical industries.

The Shift to Next-Gen Encryption (NGE)

Next-Gen Encryption provides a security level of up to 256 bits, significantly higher than today's 128-bit standard. Integrated into Internet Engineering Task Force (IETF) standards, NGE algorithms create a secure, interoperable foundation that facilitates collaboration in environments where costs or logistics have traditionally hindered information sharing for business, government, and military use.

NGE also supports public and private sector organizations that need to meet compliance requirements, including the Payment Card Industry Data Security Standard (PCI DSS) for retail, the Health Insurance Portability and Accountability Act (HIPAA) for healthcare, and the Federal Information Processing Standards 140-2 (FIPS), among others.

Next-Gen Encryption secures information travelling over networks using well established, public-domain cryptographic algorithms:

- Encryption based on the Advanced Encryption Standard (AES) using 128- or 256-bit keys
- Digital signatures with the Elliptic Curve Digital Signature Algorithm (ECDSA) using curves with 256- and 384-bit prime moduli
- Key exchange, either pre-shared or dynamic, using the Elliptic Curve Diffie-Hellman (ECDH) method
- Hashing (digital fingerprinting) based on the Secure Hash Algorithm-2 (SHA-2)

The use of public-domain algorithms simplifies adoption, strengthens the overall architecture security, and minimizes operational costs.

Other encryption solutions have been promoted from time to time, for example, Quantum Key Distribution (QKD). This encryption system relies on the transmission of individual photons from the encryption device to the decryption device. It does not depend on any computational assumptions such as the conjectured difficulty of factoring the product of two large prime numbers. While this novel approach has garnered a certain amount of attention in the press, QKD brings considerable drawbacks to the table. It works only over a limited range at a limited data rate, it cannot be used in mobile networks or devices, and it requires its own physical layer, adding complexity to the network.

Industry Best Practices with Advanced Encryption

By relying on advanced encryption such as NGE, a variety of industries are able to protect their data in today's rapidly transforming "any-to-anywhere" environments.

Public Sector: Government organizations are migrating rapidly into the cloud and mobile environments with the growing use of networked citizen services. These systems also require more large-scale data centers. However, agencies are increasingly the target of hacker attacks. Advanced encryption keeps government organizations in compliance with the FIPS 140-2 and IRS 1075 standards, as well as helping to meet security requirements for citizen data confidentiality.

Public Safety: Local and state public safety organizations increasingly depend on mobile networking for data sharing in emergency situations. Wireless devices in police, fire, and medical vehicles connect to a network backbone to enable rapid disaster response and coordination. However, relying on wireless data transmission also increases the possibility of interference with or attacks upon critical data. Cisco encryption protects data traversing these wireless backhaul links to protect information during emergencies. It also secures routine data within the overall infrastructure for regular office communications.

Finance: Today's financial organizations are faced with increased regulation of information security, while at the same time needing to meet growing customer demand for secure mobile and wireless transaction capabilities. Advanced encryption protects ATMs, kiosks, and bring your own device (BYOD)-based transactions, helping to assure compliance with regulatory requirements. Companies avoid the financial penalties and lower consumer confidence engendered by data breaches.

Healthcare: To meet HIPAA requirements, today's healthcare organizations are sharing confidential patient information between hospitals, out-patience clinics, doctors' offices, labs and special units, and the patient's bedside. Advanced encryption allows this expanding network to comply with regulatory standards for medical data, while protecting in-house hot spots and wireless networks.

Retail: Today's stores are managing complex environments based on strong trends toward mobile shopping, online shopping, and in-store use of Wi-Fi hot spots. As well, employees and management are relying on mobile devices to provide up-to-date information and manage customer concerns. Advanced encryption keeps the retailer in compliance with PCI security standards while protecting Internet access, social media, use of Q-codes, and other online activities.

Cisco Next-Generation Encryption

Cisco NGE leads the industry in advanced encryption, providing support for Suite B and 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.

NGE's algorithms are based on more than 30 years of global advances and evolution in cryptography, supported by extensive, broad-ranging academic and community review. Cisco NGE:

- Helps meet business and regulatory requirements for a variety of industries
- Uses upgraded algorithms, key sizes, protocols, and entropy to meet security requirements up to AES 256
- Offers a complete algorithm suite in which each component provides a consistently high level of security
- Can effectively scale to meet high throughput and large numbers of connections
- Can scale down to meet the security needs of low-power devices while supporting efficient battery use
- Is included in international protocols developed by bodies such as the IETF, IEEE, and Wi-Fi Alliance and standards such as IPSec, TLS, MACSec, etc.

- Is applied to the Internet Key Exchange Version 2 (IKEv2) and Transport Layer Security (TLS) Version 1.2.
- Continues to support older algorithms to help ensure backward compatibility

Companies can use Cisco's NGE to lay the groundwork for future security and scalability needs while meeting current encryption requirements.

The NGE-Based Encrypted Network

The Cisco NGE encrypted network is based on virtual private network (VPN) technology. VPNs 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 through the use of dedicated connections and encryption.

Ten years ago, SSL-based VPNs were perceived as inflexible, complex, and difficult to deploy. However, dramatic advances have transformed the segmentation approach into one of the most dynamic security options available. VPN solutions are now available for most of today's topologies, including mobile environments. The encrypted VPN is designed to:

- Secure traffic using NGE and authentication
- Connect remote users to each other and to the network
- Quickly add new sites or users, without impacting existing infrastructure
- Improve productivity by extending corporate networks, applications, tools
- Reduce communications costs while increasing flexibility
- Provide secure management capabilities
- Enable secure wireless functions

Cisco VPNs include:

- Site-to-Site Encrypted VPNs for reliable, high-quality transport of complex, mission-critical traffic over an Internet-based WAN infrastructure to branches, home offices, and business sites
- 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 the mobile network
- Group Encrypted Transport VPNs (GET VPNs) for large-scale video and voice support
- Dynamic Multipoint VPNs (DMVPNs) for centralized management of mobile environments

Conclusion

A leader in cryptography and security, Cisco encrypted networks offer significant benefits across today's vital industries and national infrastructures. Your organization becomes future-ready with more efficient security, significant cost savings, and improved ability to stay ahead of bad actors—even at a time when your data is becoming more unsafe every day. Cisco NGE:

- Supports a new range of algorithms to help secure data traffic for the next generation
- Connects remote users to each other and to the network
- Enables more secure management capabilities and wireless functions across the network instead through each application
- Quickly adds new sites or users, without impacting existing infrastructure
- Improves productivity by extending corporate networks, applications, and tools

To learn more about Cisco NGE, please contact your Cisco representative.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

Printed in USA C11-728371-00 05/13