END-OF-LIFE NOTICE, NO. 1118

CET-CISCO ENCRYPTION TECHNOLOGY END-OF-LIFE ANNOUNCEMENT

OVERVIEW

This Product Bulletin announces the End-of-Life of Cisco® Encryption Technology (CET), the 40- and 56-bit Data Encryption Standard (DES) network layer encryption available since Cisco IOS® Software Release 11.2. The last Cisco IOS images supporting CET will be Cisco IOS Release 12.1 and certain 12.1 early deployment images. These releases will remain fully supported by the Technical Assistance Center (TAC) for a minimum of two years from the date of this announcement or until End of SW Maintenance Support of Cisco IOS Release 12.1. CET will be removed effective the next major Cisco IOS mainline and early deployment release (subsequent to Cisco IOS Release 12.1). In addition, all existing 12.0 and earlier Cisco IOS images with CET will continue to be available for customers already using the feature.

CET appears in images with the following naming conventions:

56, e.g., ENTERPRISE PLUS 56

40, e.g., ENTERPRISE PLUS 40

IPSec 56, e.g., ENTERPRISE PLUS IPSec 56

IPSec 3DES, e.g., ENTERPRISE PLUS IPSec 3DES

Customers who wish to add network layer encryption in the future should deploy the Internet Engineering Task Force (IETF) standard IPSec (IP Security) instead of CET. While specific CET images will no longer be available in release 12.1, CET will continue to be included as part of the IPSec images. This enables a smooth migration for customers using CET to move to the standards-based IPSec with a simple software configuration change. Cisco IOS IPSec images are identified by “IPSec” in the image description and by “56i” or “k” in the image name. Current CET customers can switch to IPSec at no additional software charge by moving to these images.

WHY WE ARE MAKING THIS ANNOUNCEMENT

Cisco has been offering CET in Cisco IOS images for several years to provide early deployment of network layer encryption. CET was introduced to address this need while there was not a standards-based alternative for encryption functionality. In light of the increasing popularity of the IPSec standards (available since Cisco IOS Release 11.3T), Cisco has decided to End-of-Life the proprietary CET feature in favor of the standards-based IPSec.

CUSTOMER TRANSITION

Customers deploying encryption solutions for the first time should deploy an IPSec solution. Existing CET customers should move to IPSec if they require new Cisco IOS features that appear in 12.1 and later images.

Transition steps include:

1. Select the new IPSec-based image from Cisco Connection Online (CCO), and review the Flash and DRAM requirements for this image.
2. Changes will be required to the CET-based configuration.
   - Add Internet Key Exchange (IKE) policy
   - Create new IPSec transform policies

- Determine which IPSec mode, tunnel, or transport is required
- Modify existing crypto maps such that the new IKE and IPSec policy suites are applied

3. Discuss and review proposed configuration changes with the local Cisco support team before applying the new configuration.
4. Insert any new encryption adapters and remove existing ESA (Encryption Service Adapter) cards.

The CET acceleration card for the 7200 and 7500 Series of routers, the Encryption Services Adapter (ESA), will continue to be fully supported. Cisco offers an upgrade program from the ESA to the Integrated Services Adapter (ISA) for customers who wish to deploy IPSec encryption across their network. Note that existing CET customers do not need to switch to IPSec at this time if they are satisfied with their current CET-based encryption deployments.

IPSec AS AN ALTERNATIVE

IPSec and the IKE provide an IETF standards-based alternative for encryption, authentication, and integrity services for IP traffic. Customer might want to migrate to the IPSec for several reasons, including:

- Standards: IPSec is an IETF standard, providing for multivendor interoperability.
- Remote access VPN: IPSec in Cisco IOS Software can be used to terminate IPSec tunnels originated on PCs or workstations. This allows secure access across the Internet for remote workers or telecommuters, greatly reducing remote access costs.
- Greater security: IPSec in Cisco IOS Software supports both 56-bit DES encryption and the highly secure 168-bit Triple DES encryption. CET supports only 56-bit DES encryption.
- Stronger authentication: IPSec in Cisco IOS Software supports digital certificates for the strongest possible user and site authentication.

More information is available on Cisco IOS IPSec at:
http://www.cisco.com/en/US/products/sw/iosswrel/tsd_products_support_category_home.html.

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

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

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica Croatia • Cyprus • Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR Hungary • India • Indonesia • Ireland • Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal • Puerto Rico • Romania • Russia Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

VS/LW8343 04/05