

Cisco PIX Firewall **VPN Accelerator** Card Plus

Overview

The VPN Accelerator Card Plus (VAC+) for the Cisco PIX[®] Firewall Series provides high-performance tunneling and encryption services suitable for site-to-site and remote-access applications. This hardware-based virtual private network (VPN) accelerator is optimized to handle the repetitive but voluminous mathematical functions required for IP Security (IPSec). Offloading encryption functions to the Cisco PIX Firewall VAC+ not only improves IPSec encryption processing, but also maintains high-end firewall performance. As an integral component of the Cisco VPN solution, the Cisco PIX Firewall VAC+ provides platform scalability and security while smoothly working with the services necessary for successful VPN deployments—encryption, tunneling, and firewall.

Advanced Encryption Standard

The Cisco PIX Firewall VAC+ adds Advanced Encryption Standard (AES) hardware acceleration to the Cisco PIX Firewall. Also known as Rijndael, AES provides a better combination of safety and speed than Data Encryption Standard (DES). Using 128-bit secret keys, AES offers

higher security against brute-force attacks than older 56-bit DES keys and can use 192-bit and 256-bit keys as well. AES is computationally more efficient than DES and can work at multiple network layers simultaneously. In October 2000 the National Institute of Standards and Technology (NIST) of the U.S. Department of Commerce selected AES as a new encryption technique for protecting computerized information. It is expected to replace DES, which was adopted by the U.S. Department of Defense in 1977.

High Performance

The Cisco PIX Firewall VAC+, which fits into a PCI slot inside the Cisco PIX chassis, encrypts data using 56-bit DES; 168-bit Triple DES (3DES); and 128-, 192-, and 256-bit AES algorithms at speeds up to 440 Mbps. A Cisco PIX Firewall equipped with a VAC+ can support as many as 2,000 encrypted tunnels for concurrent sessions with mobile users or other sites. In addition to encryption, the card handles numerous other IPSec-related tasks—hashing, key exchange, and storage of security associations—freeing the Cisco PIX Firewall main processor and memory to perform other perimeter security functions.



- *Encryption*—Encryption is a CPU-intensive process, potentially affecting firewall performance in high-throughput configurations. The Cisco PIX Firewall VAC+ makes it possible to send DES, 3DES, or AES encrypted data at high speeds while still providing the full range of perimeter security services available from the Cisco PIX Firewall.
- *Authentication*—RSA and Diffie-Hellman are CPU-intensive protocols that are used when a new IPSec tunnel is established. RSA authenticates the remote device, while Diffie-Hellman exchanges keys that will be used for encryption. The Cisco PIX Firewall VAC+ implements these protocols in specialized hardware, ensuring fast tunnel setup and high overall encryption throughput.
- *Tunneling*—Cisco PIX Firewall and the Cisco PIX Firewall VAC+ support the IPSec tunneling protocol, enabling high-performance, flexible network designs for both remote-access and site-to-site VPNs. Site-to-site solutions can be designed with a Cisco PIX Firewall, with combinations of Cisco PIX Firewall and Cisco VPN appliances, or with VPN-enabled multiservice routers. Remote-access solutions can use the Cisco VPN client or other third-party clients that support the IPSec tunneling protocol.

Increased Security

The Cisco PIX Firewall VAC+ provides an extra level of security by segregating sensitive VPN information from standard system processing. Onboard memory and processors handle encryption, authentication, and key-generation mechanisms. A hardware random-number generator provides high-quality input to cryptographic functions, resulting in strong security while ensuring high throughput during process-intensive rekeying operations.

Easy Implementation

A Cisco PIX Firewall automatically detects the presence of the Cisco PIX Firewall VAC+ and transfers encryption activities to the VAC+ without configuration changes. Throughput is enhanced through the use of specialized hardware that performs the complex mathematical transformations necessary to generate keys, authenticate devices, authenticate packets, and encrypt and decrypt data. The Cisco PIX Firewall VAC+ is fully compatible with network-layer IPSec and the Layer 3 encryption software services of Cisco PIX Firewall Software.

Performance Summary

- 3DES SHA-1 throughput: 305 Mbps @ 300-byte packets
- 3DES SHA-1 throughput: 440 Mbps @ 1,400-byte packets
- AES128 SHA-1 throughput: 340 Mbps @ 300-byte packets
- AES128 SHA-1 throughput: 535 Mbps @ 1,400-byte packets
- AES256 SHA-1 throughput: 300 Mbps @ 300-byte packets
- AES256 SHA-1 throughput: 440 Mbps @ 1,400-byte packets
- Simultaneous VPN tunnels: 2,000

System Requirements

- Operating system: Cisco PIX OS Release 6.3(1) or later (with DES or 3DES/AES license)
- Platforms: Cisco PIX 515/515E, 520, 525, 535 (limit one per chassis)



Standards Support

- Protocols: IPSec, Internet Key Exchange (IKE), PKCS #11
- Symmetric algorithms: 56-bit DES; 168-bit 3DES; 128, 192, and 256-bit AES
- Hashing algorithms: MD-5, SHA-1
- Asymmetric algorithms: RSA, Diffie-Helman, DSA

Technical Specifications

- Processor: Broadcom BCM5823
- PCI interface: 64-bit, 66-MHz PCI v2.1 (short form)

Environmental

Operating

- Temperature: 32° to 122°F (0° to 50°C)
- Relative humidity: 10% to 90% noncondensing

Nonoperating

- Temperature: 32° to 158°F (0° to 70°C)

Power

- 5W

Dimensions and Weight

- Height: 5 in. (10.7 cm)
- Depth: 6.5 in. (17.5 cm)
- Weight: .5 lb (.2 kg)

Certifications

Safety

- UL 1950, CSA C22.2 No. 950, EN 60950, IEC 60950, AS/NZS3260, TS001, IEC60825, EN 60825, 21CFR1040

EMI

- CFR 47 Part 15 Class A (FCC), ICES 003 Class A with UTP, EN55022 Class A with UTP, CISPR 22 Class A with UTP, AS/NZ 3548 Class A with UTP, VCCI Class A with UTP, EN55024, EN50082-1 (1997), CE marking, EN55022 Class B with FTP, CISPR 22 Class B with FTP, AS/NZ 3548 Class B with FTP, VCCI Class B with FTP

Ordering Information

PIX-VAC-PLUS	IPSec hardware VAC+
PIX-515-VPN-3DES	Cisco PIX 515/515E 3DES/AES VPN feature license
PIX-VPN-3DES	3DES/AES VPN feature license
PIX-VPN-DES	56-bit DES IPSec VPN feature license

Export Considerations

The Cisco PIX Firewall VAC+ and associated software may be export controlled.

For more information, visit:

<http://www.cisco.com/www/export/crypto/>

For specific export questions, contact export@cisco.com.

Additional Information

For more information about the Cisco PIX Firewall, visit:

<http://www.cisco.com/go/pix>



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.
Capital Tower
168 Robinson Road
#22-01 to #29-01
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 Web site at www.cisco.com/go/offices

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia
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

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Aironet, Catalyst, Cisco, Cisco IOS, Cisco Systems, the Cisco Systems logo, EtherChannel, SMARTnet, and SwitchProbe are registered trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company.
(0301R) TS/LW4130 01/03