Cisco ASR 1000 Series IPsec

Executive Summary

The Cisco® ASR 1000 Series Aggregation Services Router product line includes security capabilities that are built into the platform and do not require service blades. Security features are viewed as integral parts of the base Cisco ASR 1000 Series product rather than as add-on service modules. Therefore, in general, features such as IP Security (IPsec), Firewall, Network Based Application Recognition (NBAR), Flexible Packet Matching (FPM) are incorporated directly into the Cisco ASR 1000 Series Embedded Services Processor (ESP) containing the Cisco QuantumFlow Processor rather than offered as optional pluggable modules or shared port adapters (SPAs). In addition, security features are expected to operate at multigigabit performance levels.

IPsec, like many other features, is integrated into the ESP, and accelerated using an onboard multithreaded, multicore, multigigabit cryptographic engine (includes software developed by Cavium Networks).

Scope

This document discusses various Cisco IOS® Software VPN solutions that you can deploy using Cisco ASR 1000 Series Routers, including the benefits that these routers add to existing VPN solution deployments.

Benefits of IPsec Encryption

IPsec encryption in converged networks offers the following benefits:

- Offers encryption of existing traditional WANs (for example, Frame Relay, ATM, and leased-line)
- Complies with Health Insurance Portability and Accountability Act (HIPAA), Sarbanes-Oxley, Basel Agreement (Europe), etc.
- Provides for migration from traditional WAN to lower-cost service (for example, Internet)
- Offers ability to use the Internet as a secondary WAN for backup, high-bandwidth, or less-critical traffic
- Extends campus and branch services to teleworkers

Overview of Existing Cisco IOS Software IPsec VPN Solutions

VPNs provide the highest possible level of security through a combination of encryption and authentication technologies that protect data traversing from unauthorized access. Organizations can take advantage of the easy-to-provision Internet infrastructure to quickly add new sites or users, and can dramatically increase the reach of their networks without significantly expanding infrastructure.

Two types of encrypted VPNs are generally used today:

1. Site-to-site IPsec VPNs
2. Remote-access VPNs

Site-to-site IPsec VPNs can be in turn divided into various VPN solutions, such as:

- Native IPsec and point-to-point IPsec
- Native IPsec coupled with point-to-point generic routing encapsulation (GRE) (also known as GRE over IPsec)
- Dynamic Multipoint VPNs (DMVPNs): IPsec coupled with multipoint GRE (mGRE) and Next Hop Resolution Protocol (NHRP)
- Group Encrypted Transport VPNs (GETVPNs): Tunnel-less VPNs for private WANs

Native IPsec VPN

A popular site-to-site VPN solution for connecting remote locations to headquarters, IPsec VPN provides advanced encryption to secure information in transit. It is the solution of choice for permanent VPN connections.

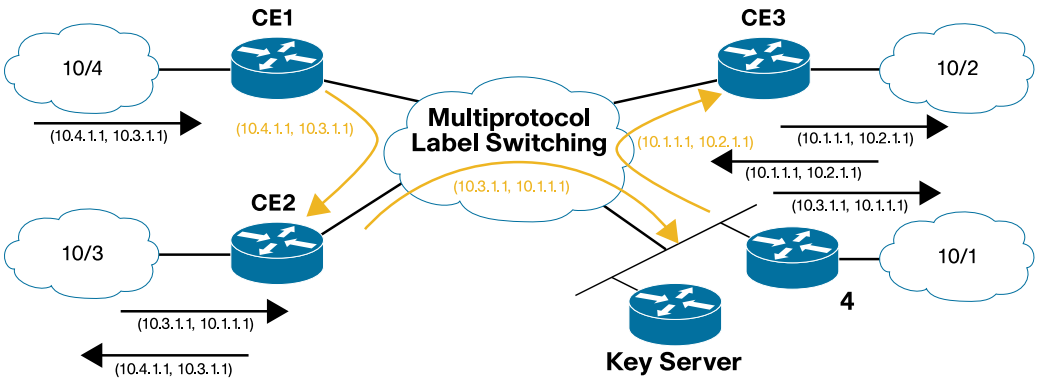
Dynamic Multipoint VPN

When branch locations want to communicate directly with each other over the public WAN or Internet (such as when using voice over IP [VoIP] between two branch offices) but do not need a permanent VPN connection between sites, Dynamic Multipoint VPN is the optimal solution.

Group Encrypted Transport VPN

When an enterprise has a private WAN network and remote locations need to communicate with each other directly, Group Encrypted Transport VPN provides optimum bandwidth efficiency while securing communications (Figure 1).

Figure 1. GETVPN: Tunnel-Less Any-to-Any VPNs: Cisco Group Encrypted VPN Solutions Provide Transparent End-to-End (customer edge-to-customer edge) Encryption



- CE1-CE4 belong to a GETVPN. All packets sent between them are encrypted with a single Services Adapter.
- The original source and destination are maintained within the MPLS cloud.

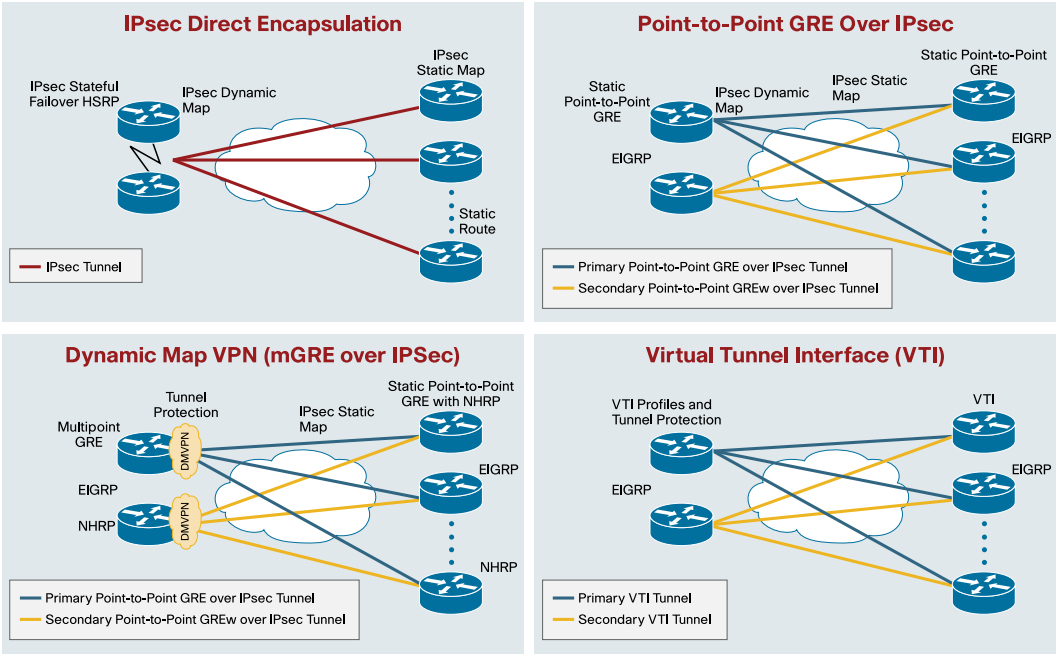
Note: GETVPN will be available on Cisco ASR 1000 Series Routers after platform general availability. For general Cisco IOS Software VPN documents, please visit http://www.cisco.com/go/vpn.

Remote VPN

For remote-access VPN solutions, the Cisco ASR 1000 Series platforms support Cisco Easy VPN. It provides secure, customizable access to corporate networks and applications by establishing an encrypted tunnel to your network whenever and wherever it is needed, securely and cost-effectively. With these solutions, you can (Figure 2):

- Enhance productivity by extending corporate network and applications
- Reduce communications costs and increase flexibility
- Provide access rights tailored to individual users, such as employees, contractors, and partners

Figure 2. IPsec VPN in the Enterprise WAN: Various Cisco IOS Software IPsec Solutions Are Available on Cisco ASR 1000 Series Routers

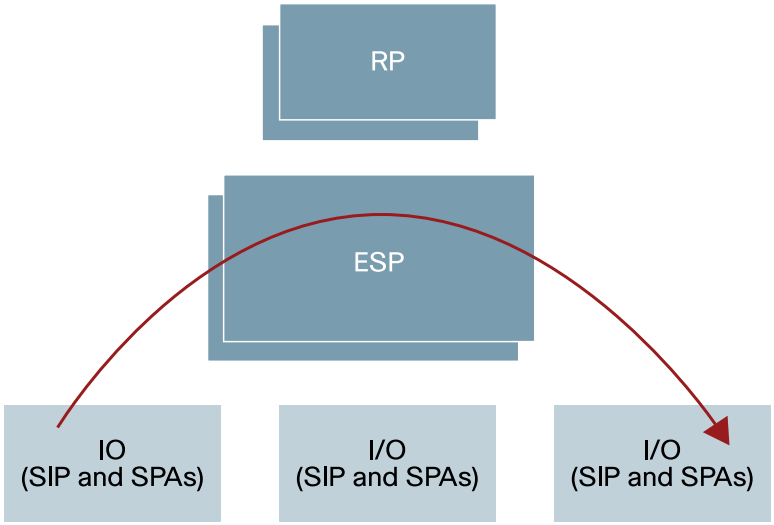


Platform Hardware Components

A Cisco ASR 1000 Series Router comprises the following functional elements in the system (Figure 3):

- **Cisco ASR 1000 Series Route Processor 1 (RP1) and Route Processor 2 (RP2):** Internet Key Exchange (IKE) packets are handled (IPsec control-plane handling) in the route processor
- **Cisco ASR 1000 Series Embedded Services Processor (ESPs):** The IPsec data plane is handled in the ESPs (encryption and decryption, IKE acceleration, etc.). The ASR 1000 Series ESPs offer three ESP models that provide different encryption performance levels (see Table 1).
- **Cisco ASR 1000 Series SPA Interface Processor (SIP):** The SIP provides housing for the SPAs; each SIP can take up to 4 half-height SPAs

Figure 3. Cisco ASR 1006 System with Dual Route Processors, Dual ESPs, and Three SIPs



Product Comparison

The following section compares the existing midrange VPN solution with new Cisco ASR 1000 Series Routers.

Table 1. Midrange VPN Solutions Comparison

	Cisco 7200 VPN Acceleration Module 2+ (VAM2+)	Cisco 7200 VPN Services Adapter (VSA)	5-Gbps ESP-5G (ASR1000-ESP5)	10-Gbps ESP-10G (ASR1000-ESP10)	20-Gbps ESP-20G (ASR1000-ESP20)
Platform Support	Cisco 7301 and 7200 Series with NPE-G2, NPE-G1 or NPE-400	Cisco 7200 Series routers with the NPE-G2	Cisco ASR 1002 Series router	Cisco ASR 1002, 1004, and 1006 Series routers	Cisco ASR 1004, and 1006 Series routers
Encryption Performance--Maximumnnp/ Internet mix (IMIX)	282 Mbps/120 Mbps	960 Mbps/600 Mbps	1.8 Gbps/1 Gbps	4 Gbps/2.5 Gbps	7 Gbps/6 Gbps
Scale (maximum number of IPsec tunnels)	5,000	5,000	4,000	4,000	4,000
Route-processor redundancy	Single route processor	Single route processor	Redundant route processor **	Redundant route processor **	Redundant route processor **
Control and data planes	Single	Single	Separate	Separate	Separate
IPsec High Availability	Box to box	Box to box	ESP to ESP	ESP to ESP	ESP to ESP
DMVPN	DMVPN Phase 3	DMVPN Phase 3	DMVPN Phase 3	DMVPN Phase 3	DMVPN Phase 3
GET VPN	Yes	Yes	Group Member (No VRF-Lite Support)	Group Member (No VRF-Lite Support)	Group Member (No VRF-Lite Support)
IPsec + IPv6	Yes	Roadmap	Roadmap	Roadmap	Roadmap
Dynamic VTIs	Yes	Yes	Yes	Yes	Yes
Quality-of-service (QoS) Preclassify	Yes	Yes	Yes	Yes	Yes
Low Latency Queuing (LLQ) before cryptographic engine	Yes	No	Yes	Yes	Yes

Cryptographic engine	Sold separately	Sold separately	Onboard	Onboard	Onboard
Quality-of-service (QoS) Preclassify	Yes	Yes	Yes	Yes	Yes
Low Latency Queuing (LLQ) before cryptographic engine	Yes	No	Yes	Yes	Yes
Cryptographic engine	Sold separately	Sold separately	Onboard	Onboard	Onboard

**Redundant Hardware route processors are available with the Cisco ASR 1006 only; redundant Cisco IOS Software (Cisco IOS Software High Availability) is available with both Cisco ASR 1002 and 1004 chassis.

The ESP, at a high level, can be divided into two subsystems:

1. Cisco QuantumFlow Processor
2. Control processor and other related circuitry

The Cisco QuantumFlow Processor--really the foundation of the Cisco ASR 1000 Series Router platform--can be further divided into two blocks: The Cisco QuantumFlow Processor, and the Cisco QuantumFlow Processor Traffic Manager. All Cisco IOS Software features are processed in the packet processor, whereas the traffic manager performs various QoS features for both traffic in transit and traffic destined to the router.

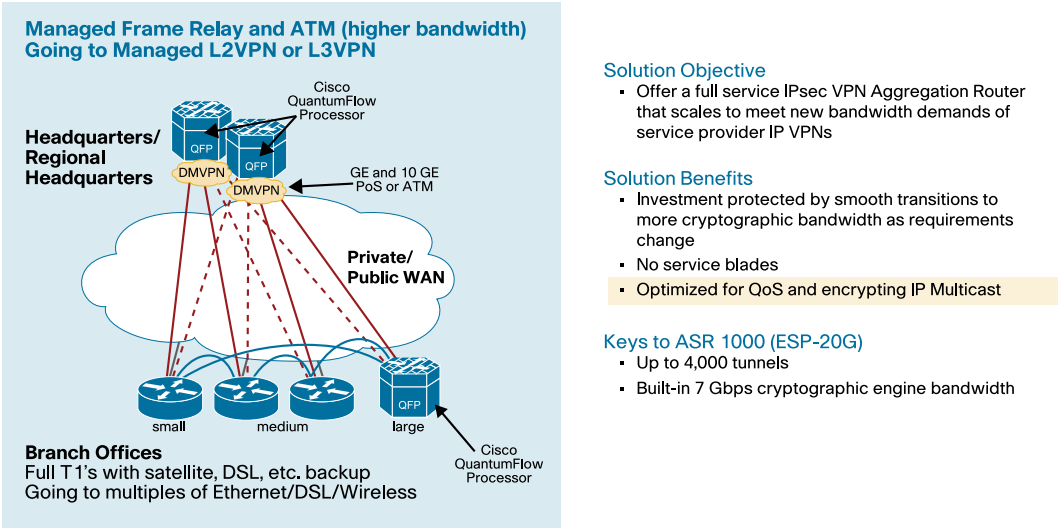
The Cisco QuantumFlow Processor achieves data-forwarding rates at tens of gigabits per second with various services configured. It includes 40 multithreaded packet-processing cores along with buffering, queuing, and scheduling subsystems (the traffic manager) to perform buffering and scheduling at wire speed.

Cisco ASR 1000 Series IPsec Solution-Specific Benefits

This section discusses some of the Cisco IOS Software VPN-related solution benefits that the Cisco ASR 1000 Series Routers add to existing solutions. Following are just a few of the innovative architectural aspects of these routers:

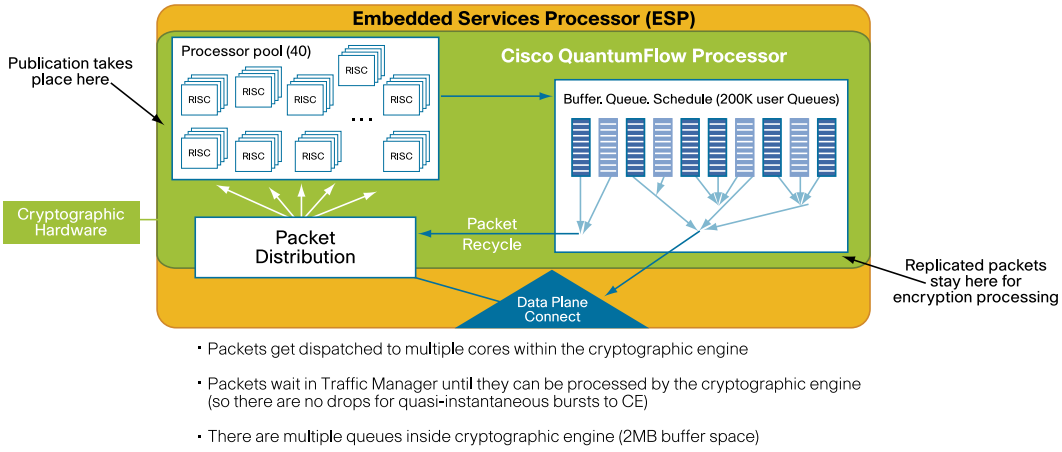
- Cisco ASR 1000 Series Routers do not require external cryptographic engine modules to perform encryption. In addition, the system bandwidth (depending on the ESP being used, 5, 10, or 20 Gbps) is available for non cryptographic traffic. For example, if you are using the 20-Gbps ESP, 6 Gbps of cryptographic bandwidth is consumed at IMIX consisting of 7 x 64B + 5 x 570B + 1 x 1500B packet sizes), and the rest of the system bandwidth (that is, 20 – 6 = 14 Gbps) remains available for passing plaintext traffic through the system (Figure 4)

Figure 4. Cisco ASR 1000 Series Routers: Multiservice, Scalable, and Secure Headend



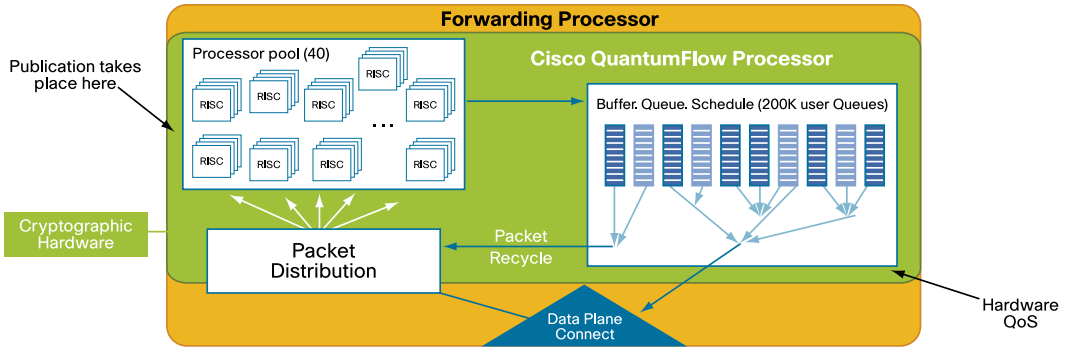
- Cisco ASR 1000 Series Routers deal innovatively compared to any router on the market with IP Multicast (IPmc) encryption to minimize any packet loss that usually happens during such processing. When multicast traffic requires encryption, the Cisco QuantumFlow Processor Traffic Manager controls packets going into the cryptographic engine, thereby avoiding any oversubscription of the cryptographic engine. Similarly, the cryptographic engine also feeds packets back into the traffic manager when it is ready to accept them (Figure 5)

Figure 5. Cisco ASR 1000 Series Sophisticated IPmc and Encryption



- Quality of service can be done at wire speeds with no performance penalty for thousands of spokes. Both pre- and post-encryption QoS are available and embedded onto the Cisco ASR 1000 Series ESP. Pre-encryption allows you to classify packets and facilitates encryption of priority traffic (such as voice over IP [VoIP]) during cryptographic engine oversubscription, whereas post-encryption with Cisco IOS Software Pre-classify allows you to classify already-encrypted packets at the egress interface based on IP/TCP/UDP headers (Figure 6).

Figure 6. Cisco ASR 1000 Series True Encryption and QoS Integration



Additional Security Benefits of the Cisco ASR 1000 Series Routers

In addition to the solution benefits from the Cisco ASR 1000 Series Routers, the platform offers several other valuable integrated security features:

- Cryptography is supported on all WAN and LAN interfaces using the standard Cisco IOS Software command-line interface (CLI), so no retraining is required for configuration
- GRE along with fragmentation are supported in the Cisco QuantumFlow Processor, resulting in much higher performance for widely used combined GRE and IPsec solutions
- In-platform forwarding line-card failover is supported between two ESPs in the Cisco ASR 1006 chassis, and no explicit configuration is required for this capability. This capability is enabled by default to preserve the IPsec state through the system in case of a failover
- Investment protection is maintained. Customers can increase encryption throughput by upgrading to a faster ESP; they can enhance IPsec tunnel setup rates by upgrading from the Route Processor 1 (RP1) to the Route Processor 2 (RP2) (note: the route processor upgrade is only applicable to the Cisco ASR 1004 and 1006 Series routers). Neither of these upgrades requires changing the existing chassis, carrier cards, and SPAs.
- Jumbo Frames are supported for encryption
- All standard ESP and HA transform sets are supported, including Message Digest Algorithm 5 with SHA-1 (MD5/SHA-1), Digital Encryption Standard and Triple Digital Encryption Standard (DES/3DES), and Advanced Encryption Standard 128, 192, and 256b (AES-128/192/256b) algorithms
- You can combine various routing and security features without significant performance degradation with VPNs, including Firewall, NBAR, NetFlow, IP service-level agreements (SLAs), etc.
- The IPsec tunnel setup rate of all the ESPs is up to 90 tunnels per second

Conclusion

Cisco ASR 1000 Series Routers are based on the innovative Cisco QuantumFlow Processor technology, which brings true integration with very good scale and performance for various Cisco IOS Software features. With the Cisco ASR 1000 Series Routers, you can deploy proper access control, Deep Packet Inspection, and threat mitigation without any additional hardware cost, design, or operational complexity as part of VPN solutions in a single, integrated platform.

Further Reading

For further information about Cisco ASR 1000 Series Router architecture, please refer to:

- Cisco ASR 1000 Series Cisco Aggregation Services Routers white paper at http://www.cisco.com/go/asr1000.
- Cisco ASR 1000 Series QuantumFlow Processor solution overview at http://www.cisco.com/go/asr1000.

Cisco Services for the Enterprise WAN Edge

Cisco and our partners help make your enterprise WAN edge deployment a success with a broad portfolio of services based on proven methodologies. We can help you establish a secure, resilient WAN architecture and successfully integrate Cisco® Unified Communications, Cisco TelePresence™, security, and mobility technologies with bandwidth to support video, collaboration, branch solutions, and growth in alignment with your business goals. Planning and design services align technology with business goals and can increase the accuracy, speed, and efficiency of deployment. Technical services help maintain operational health, strengthen software application functionality, solve performance issues, and lower expenses. Optimization services are designed to continually improve performance and help your team succeed with new technologies. For more information, visit http://www.cisco.com/go/services.

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 C22-450825-03 03/11