Network Security Features for Cisco ASR 1000 Series Routers

This data sheet provides an overview of the network security features available on Cisco® ASR 1000 Series Aggregation Services Routers.

Product Overview

Business application adoption is happening much more quickly today than five years ago. As business demands have intensified and technology has advanced, the network has evolved from a basic connection utility to a service-delivery platform.

More and more, enterprise headquarters need to extend WAN and metropolitan-area network (MAN) services globally in a rapidly evolving environment, without risking security, performance, and network uptime. Meeting those needs while minimizing operational complexity and cost is an ongoing challenge. An integrated architectural approach can help address this challenge.

In order to help enable this trend, Cisco integrated router security delivers comprehensive security services, intelligently embedding routing and security functions for fast, scalable delivery of mission-critical business applications.

Cisco ASR 1000 Series Routers offer cost-effective yet scalable WAN and MAN services aggregation integrated with security, facilitating secure extension of business resources to remote sites, business partners, teleworkers, and mobile workers. Figure 1 shows the portfolio of Cisco ASR 1000 Series Routers.

Figure 1. Cisco ASR 1000 Series Router Portfolio

The Cisco ASR 1000 Series Router is the industry's first highly scalable WAN and Internet edge router platform that delivers embedded hardware acceleration for Cisco IOS® Software services such as VPN, firewall, Network-Based Application Recognition (NBAR), NetFlow, quality of service (QoS), IP Multicast, access control lists (ACLs), Reverse Path Forwarding (RPF), and Policy-Based Routing (PBR), without the need for separate service blades. In addition, the Cisco ASR 1000 Series Router is designed for business-class resiliency, featuring redundant route processors and embedded services processors, as well as software-based redundancy. With routing performance and IP Security (IPsec) VPN and firewall acceleration up to 20 times that of previous midrange aggregation routers with services enabled, the Cisco ASR 1000 Series Routers provide a cost-effective approach to meet the latest services aggregation requirement, accomplished while taking advantage of existing network designs and operational best practices.

Powered by the Cisco Flow Processor—the industry's first scalable and programmable application-aware network processor—Cisco ASR 1000 Series Routers combine WAN and MAN services aggregation with network security features, offering customers the following benefits:

- Highly scalable site-to-site and remote-access VPN aggregation with advanced QoS and IP Multicast integration
- Advanced perimeter security, application visibility, and high-speed logging
- Detection of and response to distributed-denial-of-service (DDoS) attacks on corporate servers and other resources
- High degree of resiliency provided by control-plane separation and protection built into the edge routers, keeping them available if they are targeted
- Architecture that will be compatible with future versions: the ability to grow additional throughput or services while retaining the platform chassis and other components
- Multiservice aggregation in a single platform, simplifying operations and reducing training costs

Application Scenarios

Scalable, Secure Multiservice Aggregation

At the headquarters aggregation site, the Cisco ASR 1000 Series is positioned between the Cisco 7200 and 7301 Routers and the Cisco 7600 Series Routers and Cisco Catalyst® 6500 Series Switches. Cisco 7200 and 7301 Routers are also based on embedded services aggregation, facilitating cost-effective WAN aggregation for small to medium-sized networks, but the performance and scalability are limited to OC-3 speeds with services running. Cisco 7600 Series Routers and Cisco Catalyst 6500 Series Switches scale to 400 million packets per second (mpps) performance and are based architecturally on add-on service blades for acceleration, implying additional cost but enabling very high scalable WAN and MAN aggregation for large enterprises.

Traditionally high-performance security services have required additional hardware—either an appliance or a service blade within a router or switch. With the innovative Cisco Flow Processor, the Cisco ASR Series Router sustains upward of up to 20 mpps with high-performance services enabled—without the need for additional hardware or service blades. This performance level represents up to 20 times the performance available on the Cisco 7200 and 7301, while achieving the reduction in complexity and cost benefits that come with network service integration.

Important highlights for multiservice aggregation deployments include:

- Embedded services architecture eliminates the need for additional service blades for network and security functions such as encryption, firewall, and QoS and paves the way for cost-effective yet highly flexible and scalable multiservice aggregation, enabling IT staffs to adapt quickly to changing WAN requirements.

- An architecture that will be compatible with future versions allows expansion of bandwidth for encryption and other services by simply replacing the Cisco ASR 1000 Series Embedded Services Processor (ESP), leaving the rest of the chassis and components intact.
- Multiservice aggregation deployments are designed for scalable and optimized QoS and IP Multicast integration with VPN, allowing large-scale voice and video integration.
- The solution offers high scalability and performance: up to 4000 site-to-site tunnels and 7 gigabits-per-second (Gbps) encryption (20-Gbps ESP [ESP20]).
- The solution offers high availability in the form of hardware redundancy (Cisco ASR 1000 Series Route Processor 1 [RP1], Route Processor 2 [RP2], and ESP) and Cisco IOS Software redundancy.

Next-Generation Branch Office and Managed Customer Premises Equipment

At remote branch offices, the Cisco Integrated Services Routers Generation 2 (ISR G2) Family, Cisco's latest addition to the tremendously successful integrated services router portfolio, has featured the Cisco 1900, 2900, and 3900 Series platforms, which provide industry-leading services integration. The Cisco ASR 1002-F and 1002 Routers extend the integration of network and security services for large branch offices and regional offices, taking the performance and scalability to a much higher level.

Important highlights for branch-office and managed customer-premises-equipment (CPE) deployments include:

- The solution supports virtually all interfaces from DS-0 to OC-192.
- It allows the branch office to route correctly over various types of Ethernet service-level agreements (SLAs).
- It optimizes the WAN to route around brownouts in the service provider network to further guarantee mission-critical applications.
- Small form factors—two rack units (2RUs)—are available; Cisco IOS Software redundancy and modularity provide enhanced robustness and keep devices manageable even when Cisco IOS Software is down.
- The solution offers ground-breaking price-performance: up to 5- or 10-Gbps firewall with Network Address Translation (NAT) and 4-Gbps IPsec, along with WAN optimization and high-performance voice and video integration.

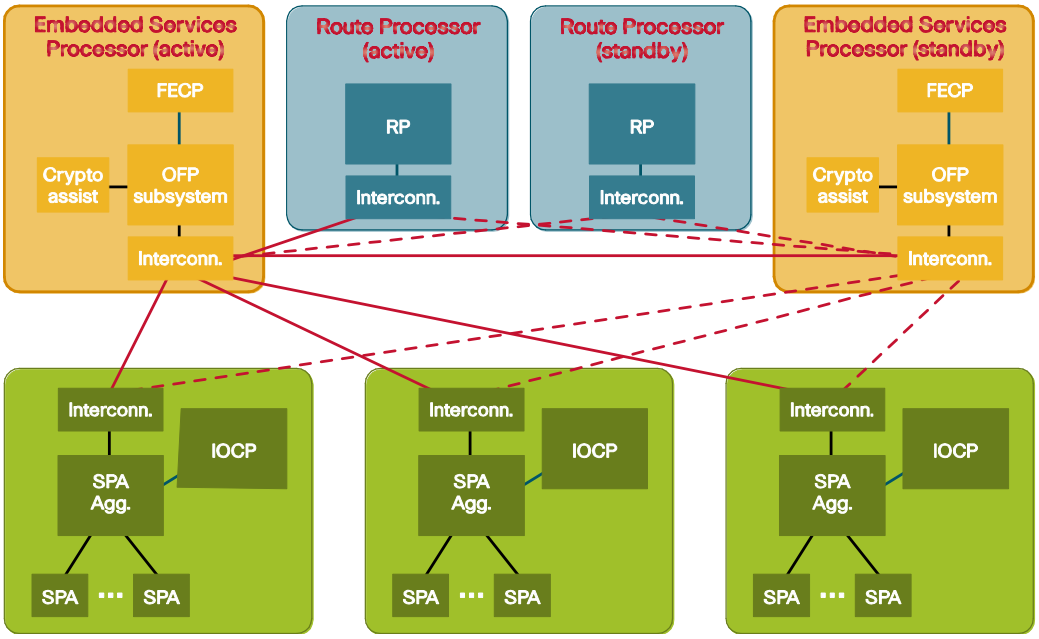
Product Architecture

The hardware architecture on the Cisco ASR 1000 Series Routers represents a significant shift away from the traditional midrange router architecture, where the management plane, control plane, and forwarding plane were all collapsed onto a single CPU—which while being highly cost-effective offered limited scalability while processing multiple services.

Cisco ASR 1000 Series Routers feature hardware separation of functions into separate processors:

- The route processor handles control-plane traffic; it implements IP routing protocols and manages the system.
- The ESP handles forwarding-plane traffic; it performs packet-processing functions such as firewall inspection, ACLs, encryption, and QoS.
- The shared-port-adapter (SPA) carrier cards house the SPAs, which provide interface (I/O) connectivity.
- Figure 2 shows the architecture for the Cisco ASR 1006 Router, featuring redundant route processors and ESPs. The Cisco ASR 1004, 1002, and 1002-F Routers have a single route processor and ESP, and redundancy is provided in software.

Figure 2. Cisco ASR 1000 Series Router Hardware Architecture



Distributed Control Plane

Cisco ASR 1000 Series Routers feature a distributed control plane; that is, every processor—whether route processor, ESP, or I/O—has its own CPU to run the various components and perform any required housekeeping, thereby freeing the route processor from having to manage the forwarding or I/O operations.

- The route-processor CPU itself runs the control plane; for example, the Interior Gateway Protocol (IGP) traffic destined for the router, traffic coming through the management port, and so on.
- Within the ESP, a control processor called the Forwarding Engine Control Processor (FECP) bootstraps the Flow Processor and cryptography chips (they include software developed by Cavium Networks), including restarting them if a failure occurs.
- Each of the SPA carrier cards has its own I/O control processor (IOCP), which performs the SPA online insertion and removal (OIR) and runs the SPA drivers.

Centralized Forwarding Architecture

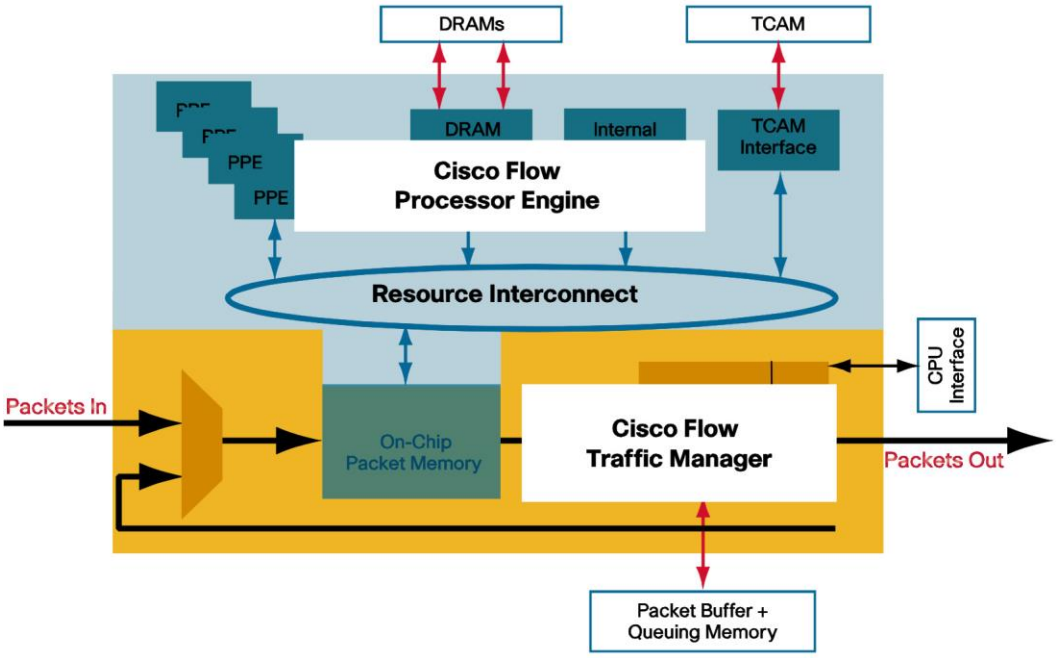
Cisco ASR 1000 Series Routers use a centralized forwarding architecture; all traffic flows through the centralized ESP, and the packet processing (firewall, ACLs, encryption, QoS, and so on) is performed there. This setup allows the administrator to configure the functions as if the router is a Cisco 7200 Series Router; for example, cryptography maps, protection, and so on can be configured just the same, without requiring hardware-specific commands.

Within the forwarding processor, however, multiple functions are implemented in parallel, allowing tremendous scale and performance.

Cisco Flow Processor

At the core of the network forwarding processor is the next-generation Cisco Flow Processor, next-generation network-processor technology that delivers true massively parallel and flexible flow processing for classification, services integration, and traffic management. Figure 3 shows a block diagram of the Cisco Flow Processor.

Figure 3. Cisco Flow Processor Major Block Diagram



The Flow Processor is not just a chip or hardware solution; it offers a next-generation hardware and software architecture that will be used in future Cisco products. In the current implementation on the Cisco ASR 1000 Series Routers, this processor contains two main pieces of silicon:

- Cisco Flow Processor Engine: The engine is a set of 40 powerful packet-processing engines (cores) running at 900 MHz to 1.2 GHz. This massive amount of parallel processing allows the entire payload and frame headers to be processed. Essentially this chip is dedicated to accelerating Cisco IOS Software features such as firewall, NBAR, and NetFlow and reduces the need for external service blades inside the router.
- Cisco Flow Traffic Manager: The traffic manager is a hardware-queuing engine with hundreds of customized network-processor resources, each capable of flexible flow processing for many applications into more than 100,000 queues anywhere in the network. This chip enables accelerated and highly scalable QoS with minimum penalty for deploying shaping, policing, and similar functions.

In addition, on- and off-chip resources on the ESP assist the Flow Processor in accelerating specific features:

- The cryptographic engine features multiple packet-processing cores to accelerate cryptographic functions, delivering up to 7-Gbps IPsec throughput. The engine is accessed from the Packet Processing Elements (PPE) by sending the packet to the traffic manager, where it is buffered, queued, and scheduled to the cryptographic engine. When the cryptographic operation is completed, the packet returns to a PPE for additional packet processing.
- Scalable IP Multicast encryption: Three mechanisms—the multiple cores in the cryptographic engine, full-circle back-pressure mechanisms between the cryptographic engine and Flow Processor, and a large cryptographic-engine buffer—are all designed to enable highly scalable IP Multicast encryption, avoiding packet drops in situations where bursts of replicated packets are directed at the cryptographic engine.

- Multigigabit performance firewall: The powerful multiple-core Flow Processor facilitates the delivery of Cisco IOS Firewall and NAT up to 20-Gbps throughput with the 20-Gbps ESP (ESP20). This performance is even sustainable with critical features such as routing, QoS, and NetFlow enabled.
- Other resources assist the Flow Processor in hardware feature acceleration of network address and prefix lookups, hash lookups, Weighted Random Early Detection (WRED), traffic policers, range lookups, and ternary content addressable memory (TCAM) for advanced classification and ACL acceleration as it processes packets.

Software Architecture: Software Redundancy

The 6-rack-unit (6RU) Cisco ASR 1006 features redundant route processors and ESPs. Each route processor can run its own copy of Cisco IOS Software, and you can configure In-Service Software Upgrade (ISSU) between them, allowing the system to recover from failure instantaneously. The 2RU Cisco ASR 1002-F and 1002 and 4RU Cisco ASR 1004 units have a single route processor and a single ESP, so hardware redundancy is not possible. Instead, high availability is provided in software:

- You can run two copies of Cisco IOS Software on a single route processor that can perform Nonstop Forwarding with Stateful Switchover (NSF SSO) between each other. For example, while the active Cisco IOS Software is building Open Shortest Path First (OSPF) adjacencies and populating the OSPF database, the standby Cisco IOS Software is kept up-to-date through interprocess communication messages. In effect, another copy of the database is readily available if the active Cisco IOS Software fails and the standby Cisco IOS Software needs to take over: the OSPF database is preserved without losing adjacencies.
- ISSU is supported for Cisco IOS Software and SPA drivers, allowing system updates without service disruption.
- Control-Plane Protection (CoPP) mechanisms performed in hardware provide maximum protection and resilience under heavy DDoS attacks, keeping the system operational and accessible by administrators.

Cisco Self-Defending Network

Cisco ASR 1000 Series Routers are integral components of the Cisco Self-Defending Network (SDN), an architectural framework that allows organizations to identify, prevent, and adapt to network security threats. The Cisco Self-Defending Network is built on Cisco Integrated Security, Cisco Collaborative Security Systems, and Cisco Adaptive Threat Defense, with Cisco Network Foundation Protection as an underlying support structure.

Cisco Integrated Security revolutionized network security by making every network element a point of defense, including routers, switches, appliances, and endpoints. The core elements of Cisco Integrated Security that enable routers to become critical devices for securing the network include secure connectivity, integrated threat control, and trust and identity.

- Secure connectivity: This feature provides secure and scalable network connectivity, incorporating multiple types of traffic. Examples include IPsec VPN, Dynamic Multipoint VPN (DMVPN), Group Encrypted Transport VPN, and Enhanced Easy VPN.
- Integrated threat control: This feature prevents and responds to network attacks and threats using network services. Examples include Cisco IOS Firewall, NetFlow, and Flexible Packet Matching (FPM).
- Trust and identity: This feature allows the network to intelligently protect endpoints using technologies such as authentication, authorization, and accounting (AAA) and public key infrastructure (PKI).

Cisco Collaborative Security Systems enable security to become a networkwide system, including endpoints, network, and policies. For example, NetFlow collectors help identify DDoS attacks quickly, and source-based Remotely Triggered Blackhole (RTBH) filtering sets up real-time defenses along all required points of attack—multiple services and devices coordinate to thwart attacks with active management.

Cisco Adaptive Threat Defense further minimizes security risks by dynamically addressing threats at multiple layers, helping enable tighter control of network traffic, endpoints, users, and applications. It also simplifies architectural designs while lowering operational costs by consolidating services onto fewer devices. This innovative approach combines secure, multilayer intelligence; application protection; networkwide control; and threat containment within high-performance solutions.

Cisco Network Foundation Protection is an integral and pervasive component of the Cisco SDN that protects the network infrastructure from attacks and vulnerabilities, especially at the network level. Examples include hardware-based CoPP and accelerated NBAR, RTBH filtering, and Unicast Reverse Path Forwarding (URPF).

Security Features and Benefits of Cisco ASR 1000 Series Routers

To enable network security features on Cisco ASR 1000 Series Routers, the following Cisco IOS Software feature sets are available:

- Advanced IP Services
- Advanced Enterprise Services

For more information about selecting the appropriate feature set, visit the Cisco ASR 1000 Router with Cisco IOS XE feature set product bulletin.

Feature licenses are required to use many of the security features on Cisco ASR 1000 Series Routers. Table 1 lists the features and corresponding feature licenses that provide entitlement.

Table 1. Security Feature Licenses for Cisco ASR 1000 Series Routers

Features	Feature License Required
IPsec, Easy VPN, DMVPN, Voice and Video Enabled VPN (V3PN), Virtual Tunnel Interface (VTI), secure provisioning and digital certificates, and IPsec High Availability	FLASR1-IPSEC-RTU
Cisco IOS Firewall and Firewall High Availability	FLASR1-FW-RTU
NBAR and FPM	FLASR1-FPI-RTU

Table 2 lists integrated security features and benefits of Cisco ASR 1000 Series Routers. Hyperlinks to additional information in this document are included for most of the features listed.

Table 2. Primary Integrated Security Features and Benefits of Cisco ASR 1000 Series Routers

Features	Description and Benefits
Secure Connectivity	
IPsec	IPsec standards supported include Digital Encryption Standard (DES), Triple DES (3DES), and Advanced Encryption Standard (AES; 128, 192, and 256) for encryption; Rivest, Shamir, Aldeman (RSA) algorithm signatures and Diffie-Hellman for authentication; and Secure Hash Algorithm 1 (SHA-1) or Message Digest Algorithm 5 (MD5) hashing algorithms for data integrity. With the built-in cryptographic engine in the ESP, the Cisco ASR 1000 Series Routers can deliver up to 7-Gbps IPsec throughput.
Hardware QoS	A dedicated QoS chip within the Flow Processor facilitates traffic shaping and policing functions for thousands of VPN spokes, as well as Low Latency Queuing (LLQ) before and after cryptography, all aimed at preserving quality of voice and real-time data.
Hardware IP Multicast handling	A powerful multicore cryptography engine with an extensive 2-Gb buffer, along with sophisticated full-circle back-pressure mechanisms between the cryptography engine and process engine, solve historical burst problems associated with high-scale IP Multicast.
Cisco Easy VPN and Enhanced Easy VPN	Providing advanced value-add to IPsec standards, these features ease administration and management of point-to-point VPNs by actively pushing new security policies from the central headend router to remote sites. Enhanced Easy VPN features integrate with dynamic VTI for maximum ease of use and advanced per-user and tunnel-specific capabilities.
Dynamic Multipoint VPN (DMVPN)	This Cisco innovation for site-to-site VPNs provides a scalable and flexible way to establish virtual full-meshed IPsecIPSec connectivity between multiple locations. DMVPN features advanced spoke-to-spoke capabilities that enhance the performance of latency-sensitive voice applications. For the traditional hub-and-spoke model, DMVPN significantly reduces deployment complexity.

Group Encrypted Transport VPN	Group Encrypted Transport VPN eliminates the need for compromise between network intelligence and data privacy in private WAN environments. Service providers can finally offer managed encryption without a provisioning and management nightmare because Group Encrypted Transport VPN simplifies the provisioning and management of VPN. Group Encrypted Transport VPN defines a new category of VPN, one that does not use tunnels.
Virtual Tunnel Interface (VTI)	You can configure these virtual interfaces directly with IPsec. VTI greatly simplifies VPN configuration and design over alternatives such as encapsulating IPsec inside generic routing encapsulation (GRE). It allows for per-user attributes and tunnel-specific features, offering administrators greater flexibility to respond to granular requirements. Both static and dynamic VTI are supported.
VRF-aware IPSec	The service connects remote sites and clients securely using IPSec to existing VPN services, such as MPLS VPN. The solution supports termination of multiple customers on the same provider edge and the ability to map it transparently to MPLS VPNs.
Secure provisioning and digital certificates	This powerful mechanism enrolls new remote nodes into the network infrastructure with maximum security.
High Availability	Cisco ASR 1000 Series Routers support several VPN redundancy options, including intrabox ESP-to-ESP IPsec Stateful Failover.
Integrated Threat Control	
Cisco IOS Zone-Based Firewall	Cisco IOS Firewall is an ideal single-device security and routing solution for protecting the WAN entry point into the network. Zone-based firewall allows grouping of physical and virtual interfaces into zones to simplify logical network topology. The creation of these zones facilitates the application of firewall policies on a zone-to-zone basis, instead of having to configure policies separately on each interface. With the powerful Flow Processor, Cisco IOS Firewall on Cisco ASR 1000 Series Routers can deliver from 2.5-Gbps up to 20-Gbps throughput.
NetFlow	NetFlow provides anomaly-based detection of DDoS attacks and supplies data that aids in tracing the attack source and reacting to the attack in real time.
NBAR	This deep inspection mechanism provides control over a wide variety of applications by recognizing and classifying them. When an application is classified, the network can then provide specific services for that application.
FPM	FPM uses flexible and granular Layer 2–7 pattern matching deep within the packet header or payload to provide a rapid first line of defense against network threats and notable worms and viruses.
High Availability	Firewall stateful failover facilitates intrabox RP-to-RP failover and ESP-to-ESP failover without losing disrupting active sessions.
Trust and Identity	
AAA	AAA allows administrators to dynamically configure the type of authentication and authorization they want on a per-line (per-user) or per-service (for example, IP, Internetwork Packet Exchange [IPX], or virtual private dialup network [VPDN]) basis.
Cisco Network Foundation Protection	
ACL	ACLs protect edge routers from malicious traffic; they explicitly permit the legitimate traffic that can be sent to the edge router destination address.
CoPP	CoPP reduces the success of a DDoS attack by policing the incoming rate of traffic to the control plane, helping maintain network availability even when under attack. CoPP is performed in hardware on the Flow Processor.
Cisco IOS Software modularity and kernel protection	Cisco IOS Software is contained within its own memory space. Even if the network is under heavy stress, for example, by a DDoS attack, the system stays operational and receptive to management.
QoS tools	QoS protects against DDoS attacks by defining QoS policies to limit bandwidth or drop offending traffic (identify, classify, and rate limit).
Receive ACLs	Receive ACLs control the type of traffic that can be forwarded to the route processor by explicitly permitting or denying traffic.
Role-based CLI access	This feature provides view-based access to command-line interface (CLI) commands, allowing highly secure, logical separation of the router between network operations, security operations, and end users.
Routing protection	This feature validates routing peers, enhances routing stability, and provides overload protection by using MD5 peer authentication and redistribution protection.
Secure Shell (SSH) Protocol Version 2	SSHv2 offers secure operator access to devices—including authentication and encryption.
Simple Network Management Protocol (SNMP) Version 3	SNMPv3 provides secure, standards-based management and control of devices for customer applications.
Source-based RTBH filtering	This feature provides wire-rate, real-time defense against DDoS attacks using a combination of IP routing features.
URPF	URPF helps mitigate problems that are caused by the introduction of malformed or forged (spoofed) IP source addresses into a network by discarding IP packets that lack a verifiable IP source address.

Secure Connectivity

Typical IP networks run innumerable applications—both legitimate and surreptitious—that compete with voice, video, and real-time data applications that are sensitive to performance. For example, voice traffic is sensitive to latency—voice packets are typically smaller, and if they are queued behind large noncritical data packets, you can immediately perceive the degradation as audible clicks. Video traffic consumes high bandwidth and is sensitive to jitter; it is often impractical to buffer video data during delays, so packets are usually dropped with a view to quickly returning to a steady stream; if this packet loss happens too often, the results are a choppy stream and unhappy viewers.

These enterprise voice and video applications require sophisticated QoS and IP Multicast mechanisms to preserve voice and video quality. The premise of site-to-site and remote-access VPNs is to transport this traffic mix over encrypted ubiquitous and inexpensive public Internet access, for both primary and backup connectivity. Extending voice and video application quality over VPNs brings additional requirements in the form of integration of IPsec with QoS or IP Multicast. In the past, some of these challenges have limited scalability or created additional complexity to network designs. Finally, as VPN adoption grows and real-time applications proliferate—voice over IP (VoIP) and IPTV are mainstream, while the popularity of Cisco TelePresence™ conferencing increases, and the adoption of video telephony is imminent—so too do the performance, scale, and feature integration requirements at the aggregation site.

Cisco ASR 1000 Series Routers deliver highly scalable, multigigabit VPNs with voice, video, and real-time data integration:

- IPsec AES, DES, and 3DES encryption is built right into the platform without the need for service blades.
- The 20-Gbps ESP (ESP20) supports up to 4000 tunnels and 7-Gbps IPsec performance.
- The architecture will be compatible with future versions, allowing additional encryption horsepower through ESP upgrades while retaining the rest of the chassis and components.
- The support site-to-site and remote-access VPNs includes IPsec, Group Encrypted Transport VPN, DMVPN, Easy VPN, and VTI (static and dynamic).
- Hardware QoS—without service blades—and sophisticated encrypted IP Multicast handling allow highly scalable designs integrating voice and video with IPsec.
- PKI features allow preshared and certificates for both site-to-site and remote access.

Hardware QoS

Cisco ASR 1000 Series Routers embed QoS processing on the Flow Processor:

- Traffic Processor: An entire piece of silicon in the Flow Processor is dedicated for QoS, facilitating traffic shaping and policing functions for thousands of spokes with virtually no effect on the route processor itself. In contrast, traditional single-CPU midrange routers would result in stress on the route processor under such conditions, potentially endangering the very availability of networks.
- LLQ before cryptography is a critical requirement to help ensure voice quality over VPNs. The Flow Processor provides hardware LLQ as well as postencryption interface-level QoS—an industry-leading capability in a platform of such scale.

Hardware IP Multicast Handling

Historically, encryption IP Multicast packets (for example, IPTV or video conferencing streams) have been possible only with limitations in scale. For example, corporate events typically start at a specified time, resulting in traffic surges when a large number of viewers attempt to join the event online at about the same time. Large numbers of packets are replicated and queued for encryption, overwhelming the queue buffers of the encryption processors and resulting in undesired packet drops at the input interface. Traditional approaches to solve this problem have involved complex designs with multiple peers and tunnels to separate encrypted IP Multicast traffic.

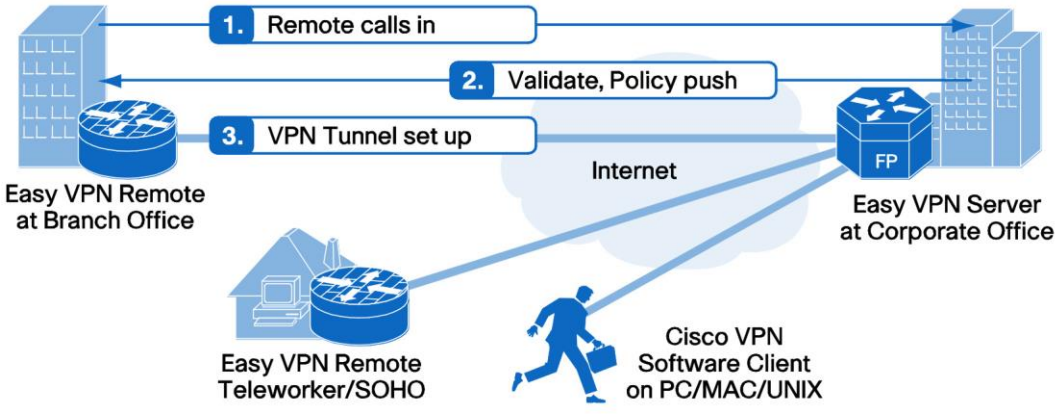
Cisco ASR 1000 Series Routers perform sophisticated handling of encrypted IP Multicast traffic. Three major provisions result in minimal packet drops and simplify network designs while encrypting IP Multicast traffic:

- Multicore cryptographic engine: The encryption processor within the ESP has multicore chips (the 10-Gbps ESP has an 8-core chip). Packets get dispatched in parallel to multiple cores for encryption, essentially packing more performance horsepower and enabling the cryptography engine to deal with a lot more packets at any given time.
- Full-circle back-pressure mechanisms between the cryptography engine and Flow Processor process engine: Traditionally, the result of quasi-instantaneous IP Multicast burst traffic has been that the forwarding and packet processor typically direct unmanageable packet bursts at each other, further taxing their buffers. Within the Cisco ASR 1000 Series Routers, multiple mechanisms allow both the cryptography engine and the process engine (the packet processing engine within the Flow Processor) to apply back pressure on each other and also to respond to back pressure by holding onto packets. This process smoothes out the burst, minimizing packet drops. The crucial element in this process is that the Flow Processor includes a dedicated traffic processor that houses the buffering, queuing, and scheduling (BQS) system, in addition to the process engine. Packets entering the system for encryption are brought into the BQS system, where they wait until the cryptography engine is ready to encrypt; that is, the cryptography engine can back pressure the process engine. When the cryptography engine is ready and encrypts the packet, it looks to reinsert the packet into the flow. The process engine in turn can now apply back pressure, asking the cryptography engine to slow down because it has no space to receive those packets. Essentially this process creates a full circle of back-pressure mechanisms between the cryptography engine and the Flow Processor.
- Large cryptography-engine buffer: The cryptography engine has a 2-MB buffer built in.

Easy VPN and Enhanced Easy VPN

For simple, high-scale, remote-access requirements, Cisco offers the Easy VPN solution, which uses a “policy-push” technology to simplify configuration while retaining rich features and policy control. Easy VPN Server, defined at the headquarters, pushes security policies to the remote VPN devices, helping ensure that those connections have up-to-date policies in place before the connection is established (Figure 4).

Figure 4. Easy VPN Tunnel Setup



Easy VPN offers the following benefits:

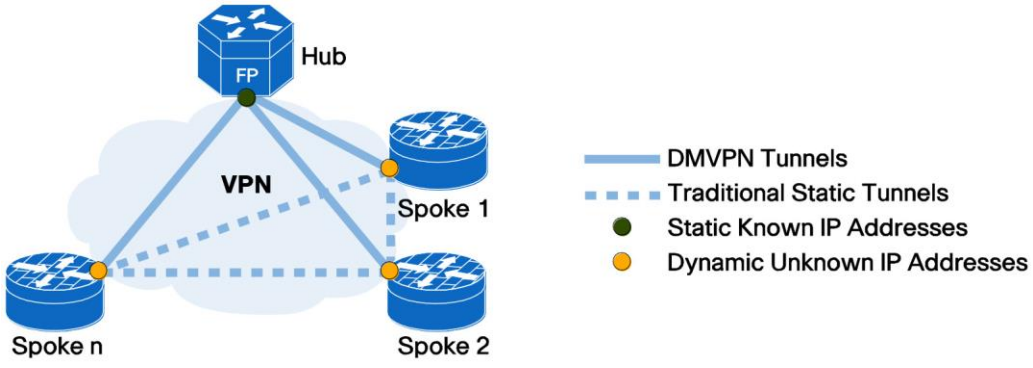
- Easy VPN supports both hardware (access routers) CPE and software remote-access clients using the same central-site router. You can install the Cisco VPN Client software on PCs, Macs, and UNIX systems to add remote-access connectivity to the router-based VPN at no additional cost. Because a single technology (Easy VPN) is used for both the hardware CPE and software clients, total cost of ownership (TCO) is reduced through simplification and unification of provisioning, monitoring, and AAA services.

- It allows local (router-based) as well as centralized RADIUS and AAA authentication of both CPE routers and individual users.
- Easy VPN supports digital certificates, improving security over preshared keys.
- It enables load balancing of multiple central-site Easy VPN concentrators. Policy push of backup concentrator information to the CPE allows you to scale the solution without CPE reconfiguration.
- The technology provides virtualization of Easy VPN Server, allowing service providers to offer VPN services to multiple customers using a single platform.
- It offers full-feature integration, including dynamic QoS policy assignment, firewall and IPS, split tunneling, and Cisco IP SLA and NetFlow for performance monitoring.
- Easy VPN is supported on all Cisco VPN product lines: Cisco IOS Software and Cisco ASA appliances.
- When you integrate Enhanced Easy VPN features with VTIs, you can configure virtual interfaces directly with Easy VPN, resulting in ease of deployment and advanced network integration. Benefits include: Greatly simplified configuration requirements at the headend as well as the remote branch offices: You can configure IP services using VTIs (or downloaded from AAA servers), and at connection time, VTI instances are cloned dynamically from these templates. There is no need to manually create myriads of similar looking sets of configuration commands for each remote site.
- Per-user attributes such as QoS: VTI allows painless configuration of policies on a per-user basis; it enables administrators to be proactive in delivering the desired application performance and keeping users productive and motivated.
- Tunnel-specific features: VTI allows for configuration of each branch-office VPN tunnel with its own set of parameters, providing flexibility to customize configuration and security based on site-specific needs.

Dynamic Multipoint VPN

Cisco routers offer DMVPN functions. Cisco DMVPN helps enable on-demand and scalable full-mesh VPN to reduce latency, conserve bandwidth, and simplify VPN deployments (Figure 5). The DMVPN feature builds upon Cisco IPsec and routing expertise by helping enable dynamic configuration of GRE tunnels, IPsec encryption, Next Hop Resolution Protocol (NHRP), OSPF, and Enhanced Interior Gateway Routing Protocol (EIGRP).

Figure 5. DMVPN



The power of DMVPN is truly reflected in the enterprise headquarters, where dynamic configuration of VPN tunnels combined with technologies such as QoS and IP Multicast optimizes the performance of latency-sensitive applications while simultaneously reducing administrative burden. For example, DMVPN allows you to obtain the same performance for voice and video applications over an IP transport network as you would over an alternate WAN link—securely and effectively.

DMVPN has been widely used to combine enterprise branch office, teleworker, and extranet connectivity. Major benefits include:

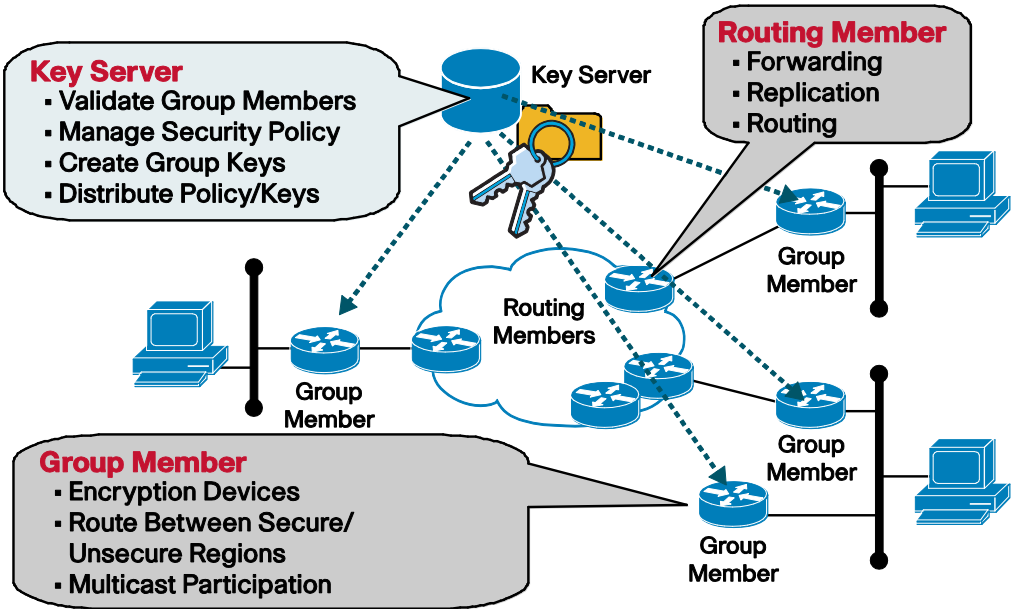
- Provides full meshed connectivity with simple configuration of hub and spoke
- Features automatic IPsec triggering for building an IPsec tunnel
- Facilitates zero-touch configuration for addition of new spokes
- Supports dynamically addressed spokes

Group Encrypted Transport VPN

With the introduction of Group Encrypted Transport VPN, Cisco now delivers an innovative, scalable category of VPN that eliminates the need for tunnels. It enables encrypted IP Unicast and Multicast packets to be routed directly to remote sites based on routing protocol decisions and to be rerouted around failed paths, providing enhanced availability. It enables organizations to rely on the existing Layer 3 routing information, thus providing the ability to address multicast replication inefficiencies and improving network performance. Distributed branch networks are able to scale higher while maintaining network-intelligence features critical to voice and video quality, such as QoS, routing, and multicast.

Group Encrypted Transport VPN offers a new standards-based IPsec security model that is based on the concept of "trusted" group members. Trusted group member routers use a common security methodology that is independent of any point-to-point IPsec tunnel relationship. A key server distributes keys and policies to all registered and authenticated group member routers (Figure 6).

Figure 6. Group Security Functions



Group Encrypted Transport VPN provides benefits to a variety of applications:

- Provides data security and transport authentication, helping to meet security compliance and internal regulation by encrypting all WAN traffic
- Enables high-scale network meshes and eliminates complex peer-to-peer key management with group encryption keys
- For Multiprotocol Label Switching (MPLS) networks, maintains the network intelligence such as full-mesh connectivity, natural routing path, and QoS

- Grants easy membership control with a centralized key server
- Helps ensure low latency and jitter by enabling full-time, direct communications between sites, without requiring transport through a central hub
- Reduces traffic loads on CPE and provider-edge encryption devices by using the core network for replication of multicast traffic, avoiding packet replication at each individual peer site

Currently, the Cisco ASR 1000 Series Routers support the Group Member and VRF-lite functionality in the Group Member.

Virtual Tunnel Interfaces

VPNs are increasingly being recognized as a mainstream solution for secure WAN connectivity. They replace or augment existing private networks that use leased lines, Frame Relay, or ATM to connect remote and branch offices and central sites more cost-effectively and with increased flexibility. This new status requires that VPN devices deliver higher performance, support for both LAN and WAN interfaces, and high network availability.

You can use the new Cisco IPsec VTI tool to configure IPsec-based VPNs between site-to-site devices. It provides a routable interface for terminating IPsec tunnels, thereby simplifying configuration. Cisco IPsec VTI tunnels provide a designated pathway across the shared WAN and encapsulate traffic with new packet headers, helping ensure delivery to specific destinations. The network is private because traffic can enter a tunnel only at an endpoint. In addition, IPsec provides true confidentiality (as does encryption), and can carry encrypted traffic.

With Cisco IPsec VTI, your enterprise can make full use of cost-effective VPNs and continue to add voice and video to your data network without compromising quality and reliability. The technology provides highly secure connectivity for site-to-site VPNs, enabling converged voice, video, and data over IP networks.

VRF-Aware IPsec

VRF-aware IPSec enables service providers to extend their MPLS VPN network services to remote branches and remote access users that belong to different enterprises. These remote locations are connected securely over IPSec VPN to the provider edge of the MPLS VPN network. The provider edgedecrypts the traffic and then forwards it using the MPLS VPN network to corresponding enterprise VPN sites. As of Cisco IOS XE Software Release 2.6, the Cisco ASR 1000 Series Routers offer two types of VRF-aware IPsec solutions: IPsec tunnels with static crypto maps, and GRE+IPSec tunnels.

High Availability and Load Balancing for the Headquarters

Cisco ASR 1000 Series Routers support several redundancy features for IPsec VPNs:

- In-box IPsec Stateful Failover: IPsec Stateful Failover allows you to employ a backup IPsec process to continue processing and forwarding IPsec packets after a planned or unplanned outage occurs. This feature is available on the 6RU Cisco ASR 1006 Routers: the IPsec Stateful Failover is between two ESPs within the same chassis. One ESP is active while the other is on hot standby, and the IPsec session information is preserved when the backup ESP takes over, without losing secure connections with its peers if the active router loses connectivity for any reason. This procedure is transparent to the end user and does not require adjustment or reconfiguration of any remote peer. IPsec Stateful Failover is designed to work in conjunction with SSO between the two ESPs with the Cisco ASR 1000 Series Router. It protects IPsec, GRE-encapsulated IPsec, and Cisco IOS Software Easy VPN traffic.

Integrated Threat Control

The Flow Processor architecture represents a radical shift in midrange router security, enabling the Cisco ASR 1000 Series Routers to deliver hardware-accelerated multigigabit integrated threat-control services combined with world-class IP routing and secure connectivity—without the need for add-on service blades.

Integrated threat-control services available initially include firewall, NBAR, NetFlow, and source-based RTBH—all proven methods used by network and security professionals to mitigate risks at the network edge.

All these functions are performed on the Flow Processor itself—all session packets, that is, Layer 4, deep packet inspection, NBAR, and FPM, are performed on the Flow Processor. Even the initial firewall session setup packets are processed in hardware in what is commonly referred to as the “fast path”—there is no “slow path” as such for firewalling. In addition, the Flow Processor performs high-speed firewall and NAT syslogging directly off the forwarding plane, minimizing any degradation or load on the route processor.

Cisco IOS Zone-Based Firewall

Cisco IOS Zone-Based Firewall on Cisco ASR 1000 Series Routers performs multigigabit stateful firewall inspection, facilitating an ideal single-box security and routing solution for protecting the WAN entry point into the network.

The firewall service is embedded in the Cisco Flow Processor within the Cisco ASR 1000 Series Routers—no additional firewall blades or modules are required. Simultaneously, the system can perform other functions such as QoS, IPv4, IPv6, NetFlow, and so on at multigigabit speeds.

Primary Cisco IOS Firewall features supported follow:

- Zone-based policies: Zone-based policies allow the Cisco ASR 1000 Series Router to act as a barrier between any interfaces that are not members of the same zone. Packets are not forwarded unless explicit zone-pair policies are specified in each direction, between each zone pair. The policy is written using Cisco Policy Language (that is, Modular QoS CLI [MQC]) and establishes the type of stateful inspection and session parameters that apply to each zone pairing. For example, the Internet-to-DMZ boundary would require an explicit policy allowing HTTP and Domain Name System (DNS) to traverse.
- Multigigabit performance: The architecture delivers firewall and NAT performance up to 2.5 Gbps on ASR 1002-F, 5 Gbps on ESP5, 10 Gbps on ESP10, and 20 Gbps on ESP20 with routing, QoS, and other common Cisco IOS Software features enabled.
- In-box high availability: The Cisco ASR 1006 supports hardware redundancy by supporting redundant route processors and ESPs within the chassis. When a fault occurs on the active route processor or ESP, the hot standby component picks up the processing with nearly zero packet loss. All firewall and NAT sessions are preserved during this process. The Cisco ASR 1002 and ASR 1004 provide software redundancy capabilities by running dual Cisco IOS Software images, one running as active and the other as standby, in a single route processor. When a fault occurs in the active image, the hot standby image picks up the process and all firewall and NAT sessions remain established.
- VRF-aware Zone-Based Firewall: It enables the Cisco 1000 as the provider edge router in the MPLS VPN network to provide firewall services to a large number of VPN customers. Each customer can have its own firewall policies. This solution offers three major use cases for VPN customers: Internet handoff, access to shared services, and site-to-site access.
- Advanced protocol inspection for voice, video, and other data applications.
- Per-user, per-interface, or per-subinterface security policies.
- Per-subscriber firewall: This solution is deployed on the Cisco ASR 1000 Series as the L2TP Network Server (LNS). This feature integrates the Cisco IOS Zone-Based Policy Firewall with the Cisco ASR 1000 Series rich

broadband feature set to enable Internet service providers to offer firewall services to their broadband subscribers.

- Tightly integrated identity services to provide per-user authentication and authorization.
- Role-Based CLI Access: This feature provides the network administrator to define different views depending on the roles of users who need access to the router. Each view includes a subset of all Cisco IOS Software CLI commands accessible to the user of a particular role, such as network operator and security operator.

NetFlow Event Logging

Cisco ASR 1000 Series Routers generate multigigabit firewall and NAT syslogs. The Flow Processor architecture of the ESP allows tens of thousands of firewall and NAT events to be exported using NetFlow v9 binary logging templates directly off the forwarding plane, without degrading the route-processor performance. The ESP can export up to 40,000 events per second.

NetFlow

NetFlow is the primary technology in the industry to detect anomalies in networks. It supplies telemetry data to analyze IP traffic—for example, who is communicating to whom, over what protocols and ports, for how long, and at what speed.

DDoS attacks create sudden spikes in network use. These spikes can be quickly identified as abnormal network "events" when compared with typical traffic patterns gleaned from previously collected profiles and baselines. By analyzing the detailed NetFlow flow data, you can also classify the attack (that is, the source and target of the attack), attack duration, and the size of packets used in the attack.

The Cisco Flow Processor on the Cisco ASR 1000 Series Routers exports huge amounts of flow cache data directly off the processor (one million flow records cards for ESP10), further reducing CPU usage of control processors in the routing platform. Sampled NetFlow results in optimized use of this cache.

Network-Based Application Recognition

NBAR is a classification engine within Cisco IOS Software that uses deep and stateful packet inspection to recognize a wide variety of applications, including web-based and other difficult-to-classify protocols that use dynamic TCP/User Datagram Protocol (UDP) port assignments. When used in a security context, NBAR can detect worms based on payload signatures. When NBAR recognizes and classifies an application, a network can invoke services for that specific application. The technology also helps ensure that network bandwidth is used efficiently by working with QoS features to provide guaranteed bandwidth, bandwidth limits, traffic shaping, and packet coloring.

Cisco ASR 1000 Series Routers accelerate NBAR right on the Flow Processor, resulting in industry-leading multigigabit performance.

Flexible Packet Matching

FPM inspects packets for characteristics of an attack and takes appropriate actions (log, drop, or Internet Control Message Protocol [ICMP] unreachable). It provides a flexible Layer 2 through Layer 7 stateless classification mechanism. You can specify classification criteria based on any protocol and any field of the traffic protocol stack. Based on the classification result, you can take actions such as drop or log on the classified traffic.

Trust and Identity

AAA

Cisco IOS Software AAA network security services provide the framework to set up access control on a router or access server. AAA is designed to allow administrators to dynamically configure the type of authentication and

authorization they want on a per-line (per-user) or per-service (for example, IP, IPX, or VPDN) basis, using method lists that are applied to specific services or interfaces.

Network Foundation Protection

Continual availability of network infrastructure devices is even more critical at the enterprise headquarters. If a network router or switch is compromised, miscreants gain complete access to the entire network. Regardless of various skillful defenses that may be employed against attacks, it is necessary to protect against the unknown.

The following technologies emphasize the importance of robust network foundation protection, including self-defense for Cisco IOS Software devices if a DDoS attack occurs and secure management access to minimize the possibility of spoofing attacks on the management and control interface.

Control-Plane Protection

Even the most robust software implementation and hardware architecture is vulnerable to a DDoS attack. DDoS attacks are malicious acts designed to paralyze a network infrastructure by flooding it with worthless traffic, camouflaged as specific types of control packets directed at the control-plane processor.

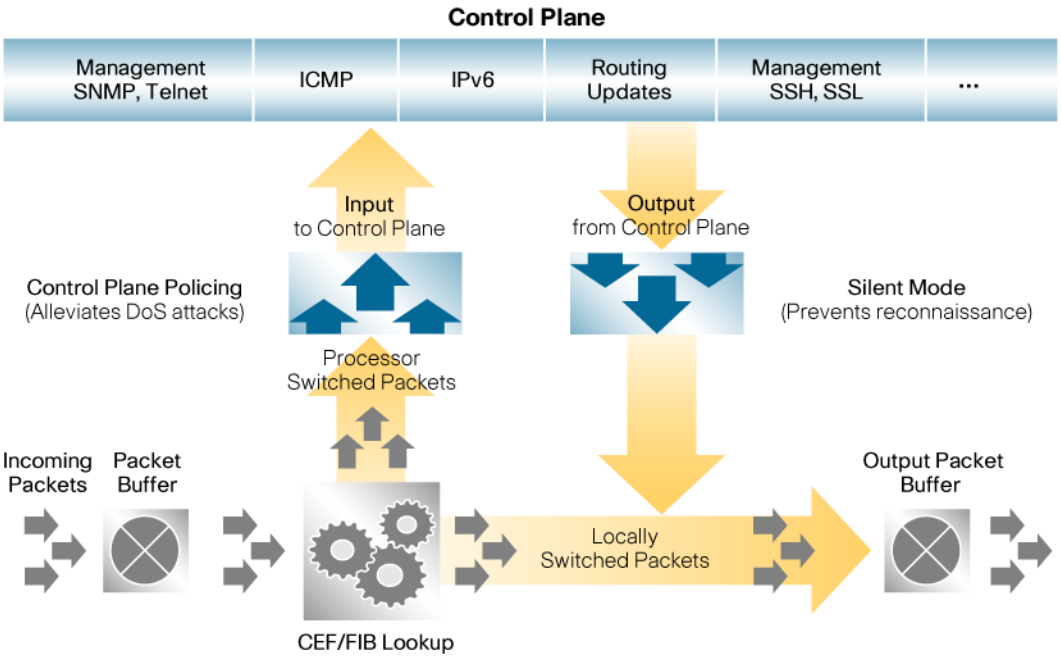
On the Cisco ASR 1000 Series Routers, the first line of defense is provided by the separation of the control and data forwarding functions in separate processors, that is, separate and dedicated CPUs on the route processor and ESP. The ESP processes the data flow; the route processor is isolated from DDoS attacks.

As a second line of defense to block this and similar threats directed at the heart of the network, Cisco IOS Software includes programmable policing functions on routers that limit the rates of, or “polices,” traffic destined for the control plane. You can configure this feature, called Control-Plane Protection (CoPP), to identify and limit certain traffic types either completely or when above a specified threshold level (Figure 7).

CoPP on Cisco ASR 1000 Series Routers is performed in hardware, on the Flow Processor, virtually eliminating any additional penalty or system degradation for performing the CoPP and rate-limiting functions. Additionally, all punt traffic in the platform goes through the ESP first, providing an additional possibility to keep deviant data from even entering the route processor.

Thirdly, running Cisco IOS Software as a user process on top of the Linux kernel provides another layer of system protection. This kernel protection allows the system to stay alive and manageable, even if the routing processes undergo stress, for example, due to DoS attacks.

Figure 7. Control-Plane Protection: Packet Buffer; Incoming Packets; Cisco Express Forwarding and Forwarding Information Base (FIB) Lookup; Output Packet Buffer; and Silent Mode



Role-Based CLI Access

Role-Based CLI Access allows the network administrator to define "views," which are a set of operational commands and configuration capabilities that provide selective or partial access to Cisco IOS Software. Views restrict user access to Cisco IOS Software CLI and configuration information and can define what commands are accepted and what configuration information is visible. Applications of Role-Based CLI Access include network administrators providing security personnel access to specific functions. In addition, service providers can use this feature to grant limited access to end customers to aid in troubleshooting the network.

SSHv2

SSHv2 provides powerful new authentication and encryption capabilities. More options are now available for tunneling additional types of traffic over the encrypted connection, including file-copy and email protocols. Network security is enhanced by a greater breadth of authentication functions, including digital certificates and more two-factor authentication options.

SNMPv3

SNMPv3 is an interoperable standards-based protocol for network management that provides secure access to devices by authenticating and encrypting packets over the network. The security features provided in SNMPv3 follow:

- Message integrity: Helps ensure that a packet has not been tampered with in transit
- Authentication: Verifies that the message is from a valid source
- Encryption: Scrambles the contents of a packet to prevent it from being seen by an unauthorized source

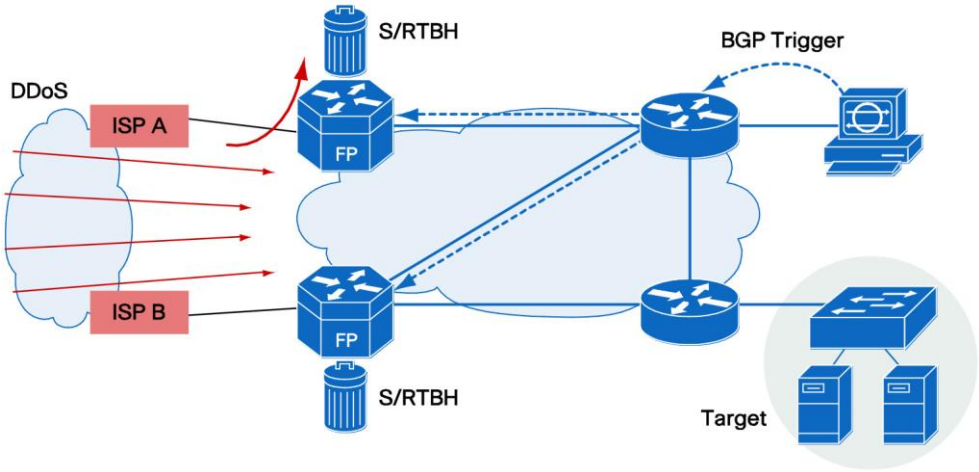
SNMPv3 provides for both security models and security levels. A security model is an authentication strategy that is set up for a user and the group in which the user resides. A security level is the permitted level of security within a security model. A combination of a security model and a security level determines which security mechanism is employed when handling an SNMP packet. Three security models are available: SNMPv1, SNMPv2c, and SNMPv3.

Source-Based Remote-Triggered Black Hole Filtering

When your organization knows where an attack is coming from (for example, by analyzing NetFlow data), you can apply containment mechanisms such as ACLs. When attack traffic is detected and classified, you can create and deploy appropriate ACLs to the necessary routers. Because this manual process can be time-consuming and complex, many customers use Border Gateway Protocol (BGP) to propagate drop information to all routers quickly and efficiently. This technique, termed RTBH, sets the next hop of the victim's IP address to the null interface. Traffic destined to the victim is dropped on ingress into the network.

Another option is to drop traffic from a particular source. This method is similar to the drop described previously but relies on the preexisting deployment of URPF, which drops a packet if its source is "invalid"; invalid includes routes to null0. Using the same mechanism of the destination-based drop, a BGP update is sent, and this update sets the next hop for a source to null0. Now all traffic entering an interface with URPF enabled drops traffic from that source. Although scalable, the BGP-triggered drops limit the level of granularity available when reacting to attack: they drop all traffic to the black-holed destination or source, as described previously. In many cases this reaction to a large attack is effective, and it certainly mitigates collateral damage (refer to Figure 8).

Figure 8. Real-Time Wire-Rate Defense Against DDoS Attacks with Source-Based RTBH Filtering



Unicast Reverse Path Forwarding

uRPF helps limit the malicious traffic on an enterprise network. It works by enabling a router to verify the reachability of the source address in packets being forwarded. This capability can limit the appearance of spoofed addresses on a network. If the source IP address is not valid, the packet is discarded. The Cisco ASR 1000 Series Routers support strict mode and loose mode.

When administrators use uRPF in strict mode, the packet must be received on the interface that the router would use to forward the return packet. uRPF configured in strict mode may drop legitimate traffic that is received on an interface that the router did not choose for sending return traffic. Dropping this legitimate traffic could occur when asymmetric routing paths are present in the network.

When administrators use uRPF in loose mode, the source address must appear in the routing table. Administrators can change this behavior with the allow-default option, which allows the use of the default route in the source verification process. Additionally, a packet that contains a source address for which the return route points to the null0 interface is dropped. An access list may also be specified that permits or denies certain source addresses in uRPF loose mode.

Ordering Information

To place an order, visit the Cisco Ordering Homepage. A comprehensive list of the Cisco ASR 1000 Series security bundles is available at www.cisco.com/go/securitybundles.

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 conferencing, 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 www.cisco.com/go/services.

For More Information

For more information about network security on Cisco ASR 1000 Series Routers, as well as the complementary Cisco 800, 1900, 2900, and 3900 Series branch-office router solutions, visit www.cisco.com/go/routersecurity or contact your local Cisco account 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 C78-452140-07 10/15