

Internet Gateway Router Design Using Cisco ASR 1000 Series Routers

Abstract

Enterprises that maintain their own networks demand intelligent routing products and cutting-edge technology for high-performance, secure, feature-rich, and affordable connectivity between headquarters and the Internet through a service provider network.

This deployment is different from WAN aggregation or a private WAN; a WAN aggregation deployment connects the enterprise to a public network, which brings with it all the requirements for the infrastructure to be very secure, service-aware, and highly available.

Selecting a product for this place in the network comes with many challenges. An ideal device needs to be flexible with regard to features and variety of interfaces, and it must be able to scale without involving a complete system upgrade or adding services modules for every necessary service. Other critical attributes include high availability and deep packet inspection (such as Network Based Application Recognition [NBAR] and Flexible Packet Matching [FPM]). High availability enables applications so they remain available in case of software or hardware failure that causes a data- or control-plane problem, whereas deep packet inspection helps classify the data based on application header or payload; it also addresses zero-day type attacks.

Internet Gateway Router Requirements

Table 1 lists the requirements for Internet gateway deployments.

Table 1. Requirements for Internet Gateway Deployments

Basic Features	Network Address Translation (NAT)	Access Control List (ACL)	Firewall	Application Availability	Network Accounting and Management
Internet Gateway Router					
Scale	5–20 Gbps with services turned on	Converged device requiring no services module for basic services	Routing- and forwarding-plane redundancy	Nonstop Routing (NSR)	
High Availability	Nonstop Forwarding with Stateful Switchover (NSF/SSO)	Scalable and modular control plane	Routing- and forwarding-plane redundancy	Performance-based routing*	Extensive network flow monitoring
High-Touch Services	NAT, VPN, deep packet inspection, and firewall with application awareness	IPv6 and related features	Stateful NAT and firewall	Performance-based routing	Extensive network flow monitoring
Interface Diversity	OC-3 and OC-12	Fast Ethernet and Gigabit Ethernet	10 Gigabit Ethernet	DS-3 and DS-1	
Infrastructure Security	Denial-of-Service (DoS) and Distributed DoS (DDoS) mitigation	Control-plane protection	Total separation of control, data, and I/O planes		

* Note: Cisco Performance Routing is not currently supported on Cisco ASR 1000 Series Aggregation Services Routers.

Internet Gateway Topologies

Consider the common topologies that are used today for this deployment (Figures 1 and 2).

Usual deployment at the head-end uses a WAN router along with several network appliances to achieve firewall and VPN functions.

Figure 1. Single Internet Gateway Router Deployment

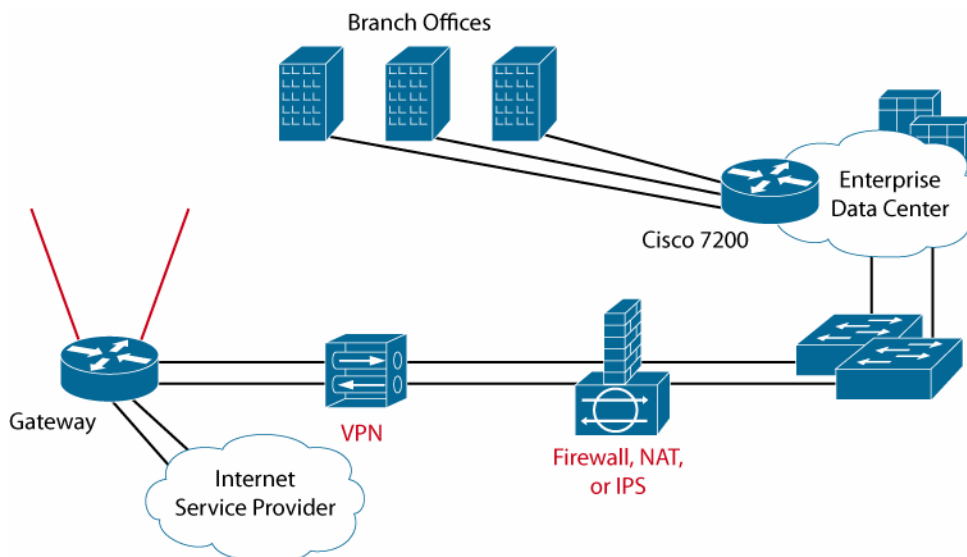
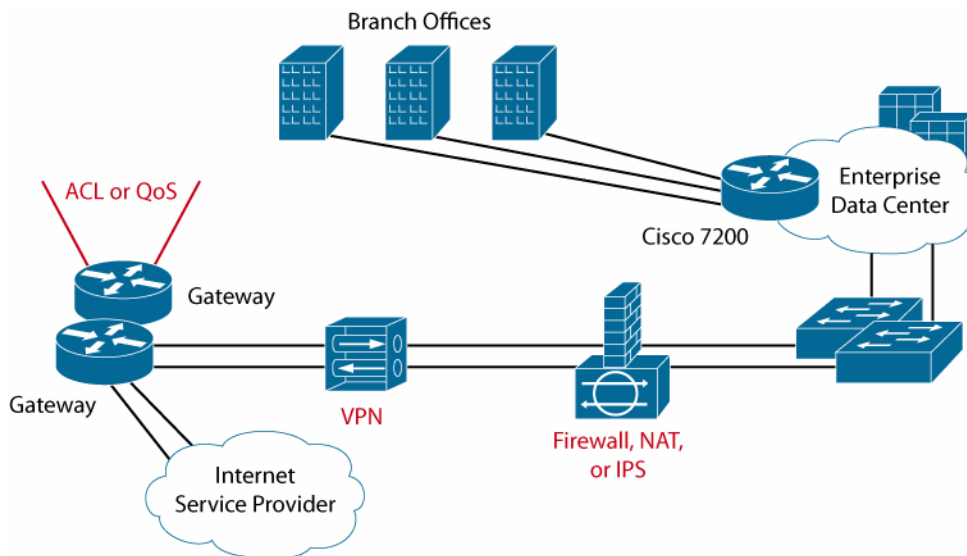


Figure 2. Dual Internet Gateway Router Deployment



The router portfolio for the Cisco Internet Gateway solution, deployed in the largest and most demanding enterprise networks worldwide, offers a wide range of connectivity options, multiprotocol support, and software features for network intelligence at high performance. Cisco Internet Gateway routers have the flexibility, scalability, and feature richness to facilitate new applications and services while delivering security, resilience, lower total cost of ownership (TCO), and ease of deployment and management.

Cisco supercharges the industry's most comprehensive class of midrange routers by introducing a new carrier-class platform of routers: the Cisco ASR 1000 Series Aggregation Services Routers. This platform brings new features and functions to the Internet gateway of the future by integrating services at 5 to 20 Gbps while at the same time increasing connectivity options.

Cisco ASR 1000 Series Routers

Cisco ASR 1000 Series Aggregation Services Routers are next-generation, modular, services-integrated routing platforms designed with the flexibility to support a wide range of 4 to 16 Mpps packet forwarding, 5 to 20 Gbps system bandwidths, performance, and scaling.

Important System Innovations

Cisco ASR 1000 Series Routers bring many innovations to the routing industry, including:

- Extremely modular, flexible, and integrated design to meet changing requirements in today's networks
- First revolutionary Cisco Packet Processor technology-based platform that facilitates various services up to 20 Gbps
- True carrier-class system design with In Service Software Upgrade (ISSU) that results in nonstop router operation
- Complete logical and physical separation of system routing, forwarding, and I/O planes, resulting in a system that is highly robust yet flexible to meet always-increasing performance needs
- Ability to store full Internet routing table on Cisco ASR 1000 Series Route Processor 1 (RP1)
- Software modularity to minimize the effects of software upgrades in the system and lower operating expenses (OpEx)
- Highly sophisticated system software and hardware design to boost application availability, even during system oversubscription
- Lights-out remote-management facility: the route processor remains accessible through a console or Ethernet management port even during Cisco IOS® Software failure
- System that reuses the investment made in network I/O by way of shared port adapters (SPAs)

Cisco ASR 1000 System Brief Overview

The Cisco ASR 1000 Series Routers address the performance gap between Cisco 7200 and Cisco 7600 Routers. This platform is fully modular from both hardware and software perspectives and has all the elements of a true carrier-class routing product serving both enterprise and service provider networks.

The Cisco ASR 1000 Series product line includes various packaging options differentiated by the number of I/O slots, capacity, redundancy, and power. A common hardware and software architecture and common components are used across these routers to support the various modular and nonmodular chassis configurations (ranging from two to six rack units). The following chassis options are available:

- Cisco ASR 1002 (2-rack unit [2RU] chassis with the modular Cisco ASR 1000 Series Embedded Services Processor [ESP] and fixed Cisco ASR 1000 Series RP1 and Cisco ASR 1000 Series SPA Interface Processor [SIP] with four built-in Gigabit Ethernet ports)
- Cisco ASR 1004 (4RU chassis with modular ESP, route processor, and SIPs)
- Cisco ASR 1006 (6RU chassis with modular and redundant ESPs, route processor, and SIPs for SPA connectivity)

Three ESPs (5 Gbps Cisco ASR 1000 Series ESP [ESP5], 10 Gbps Cisco ASR 1000 Series ESP [ESP10], and 20 Gbps Cisco ASR 1000 Series ESP [ESP20]; part numbers ASR1000-ESP5, ASR1000-ESP10, and ASR1000-ESP20 are available) provide 5 to 20 Gbps of system bandwidths.

The performance and scaling of the Cisco ASR 1000 Series Routers for a forwarding plane-bounded feature are dictated by the capability of their central forwarding engine in the form of an ESP card. Different ESP options are provided for all the chassis to give you cost, performance, and scaling choices.

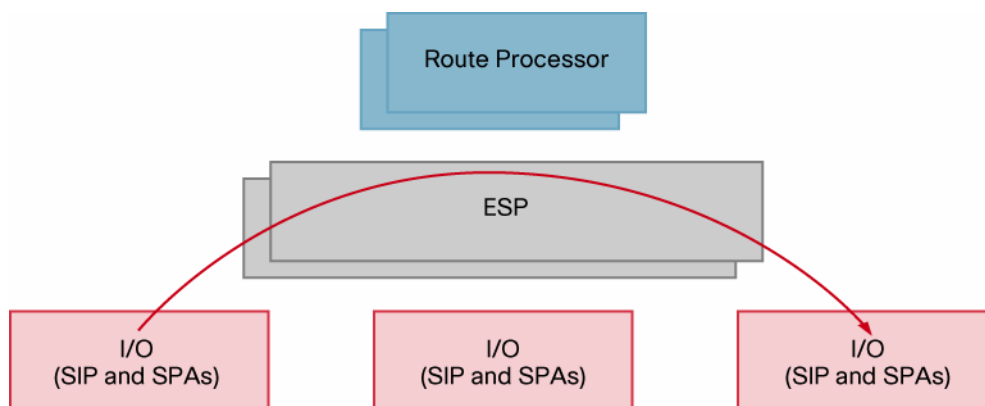
For enterprises, the Cisco ASR 1000 is intended as the midsize aggregation and gateway product, typically residing in a regional WAN or WAN edge or large branch office and providing throughput in the 5 to 20 Gbps range with various services turned on.

High-Level System Architecture and Partitioning

The Cisco ASR 1000 Series Router from a very high level can be partitioned into three elements: network control (route processor), data-plane forwarding (ESP), and network I/O (SIP). Figure 3 shows the Cisco ASR 1006 Router with two route processors, two ESPs, and three SIPs.

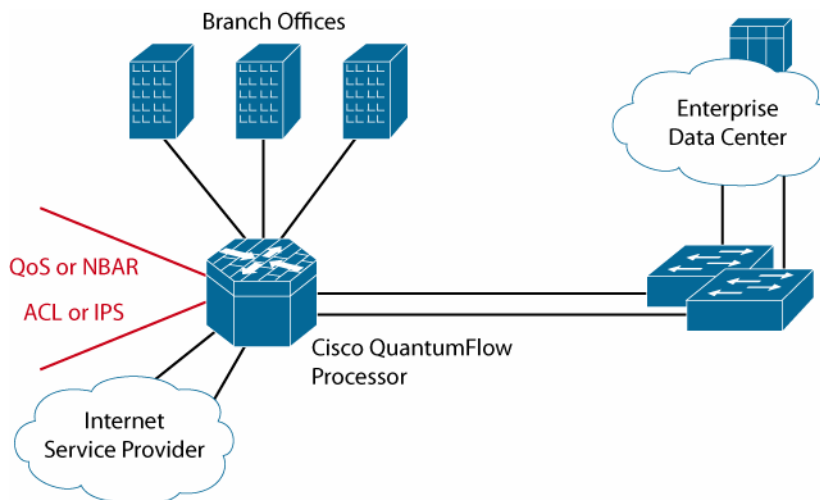
One of the main differentiators of the platform is the logical and physical isolation of these planes in the system for nonstop operation and various types of resilience. For example, the routing plane is completely isolated from the forwarding plane (in fact, they are separate cards); hence loading of one does not affect the other.

Figure 3. Cisco ASR 1006 Router with Two Route Processors, Two ESPs, and Three SIPs



With Cisco ASR 1000 Series Routers, multiple high-touch services and functions can actually be collapsed into one device (Figure 4).

Figure 4. Multi-Service Edge Deployment that Can Collapse WAN Aggregation and Internet Gateway Function on a Single Cisco ASR 1000 Series Router



In most scenarios, a single Cisco ASR 1006 Router should be able to achieve the desired high availability, resilience, and redundancy for both WAN aggregation and Internet gateway function on one sheet metal.

The following sections discuss each of the gateway router requirements and how the Cisco ASR 1000 Series Routers not only meet but exceed them.

Basic Features and High Availability

Cisco ASR 1000 Series Routers provide multigigabit Network Address Translation (NAT) and Port Address Translation (PAT) performance up to 20 Gbps to meet the mid- to high-end requirements for Internet gateway functions. NAT application awareness for protocols includes Skinny Client Control Protocol (SCCP), Session Initiation Protocol User Datagram Protocol (SIP UDP), H.323, Domain Name System (DNS), Real Time Streaming Protocol (RTSP), etc.

Cisco ASR 1000 Series Routers also bring innovations to the existing implementation to enhance the high-availability and resilience aspects.

- Stateful ESP-to-ESP NAT, firewall, and IP Security (IPSec) high availability is available to maintain nonstop NAT and firewall operation in case of a data-plane hit when one ESP goes down. Every completed NAT or firewall session gets replicated to the standby ESP in the same chassis to achieve this behavior.
- The Cisco QuantumFlow Processor provides the complete NAT session setup processing, including application layer gateways (ALGs). All Layer 4 to Layer 7 zone-based firewall session processing takes place inside the Cisco QuantumFlow Processor, hence achieving up to 5, 10, and 20 Gbps performance. This setup also frees the route processor in the system to continue control-plane processing.
- High-speed NAT and firewall translation logging is available through NetFlow Event Logging (NEL). NEL uses NetFlow v9 templates to log binary syslog to NEL collectors, allowing not only the use of NAT at multigigabit rates, but also the ability to record NAT and firewall session creation and teardown records at this speed.
- Cisco IOS Software Embedded Event Manager (EEM) is a powerful ally for device and system management available at first customer shipment (FCS). EEM enables customers

to harness the network intelligence intrinsic to Cisco IOS Software and customize the behavior based on real network events as they happen.

- Simple Network Management Protocol Versions 1, 2c, and 3 (SNMPv1, v2c, and v3) all are supported at FCS for robust and backward-compatible network management operations.
- An extensive IPv6 feature set is supported at FCS. It includes global unicast, global multicast, link local addresses, v6-to-v4 tunnels, IP Multicast Version 6, Open Shortest Path First Version 4 (OSPFv4), and MIB support.

You can use Cisco Feature Navigator to get details of all NAT- and firewall-related features for the Cisco ASR 1000 Series Router.

Scale

Cisco ASR 1000 Series Routers provide various price-to-performance options for scaling NAT up to 20 Gbps.

NAT performance is a function of the Cisco ASR 1000 ESP in the system, and the ESP is available to all chassis options as a fully modular, field-replaceable unit (FRU) component. Thus the Internet gateway design will be compatible with future versions, and you can start with ESP5 and eventually scale up by just upgrading the ESP.

The ESP10 supports up to 500,000 concurrent NAT sessions and up to 20,000 sessions per second.

Table 2 compares firewall, NAT, and IPSec performance and scale for the ESPs.

Table 2. Firewall, and IPSec Performance and Scale for ESPs

Feature	ESP5	ESP10	ESP20
Firewall	5 Gbps	10 Gbps	20 Gbps
NetFlow	500,000 flow records	1,000,000 flow records	2,000,000 flow records
IPSec	4,000 tunnels*	4,000 tunnels*	4,000 tunnels*
	Up to 90 tunnels/second	Up to 90 tunnels/second	Up to 90 tunnels/second

* Note: The 4000 number has been tested internally, but does not represent a hardware limitation. Hardware is capable of supporting way beyond that number.

High-Touch Services

Cisco ASR 1000 Series Routers accelerate most of the high-touch services using the ESP.

Relevant services at this place in the network include:

- Firewall
- IPSec
- QoS
- NBAR and FPM
- Generic routing encapsulation (GRE)
- Full and sampled NetFlow

QoS is supported at multigigabit rates without any significant degradation to other data plane-bounded functions, and no degradation to control plane-related features.

Cisco ASR 1000 Series Routers set a new benchmark with the integrating of security and routing and many more services into single router data plane, hence resulting in an extremely service-rich router family with a 10 Gbps footprint even at 2-rack units.

Interface Diversity

Cisco ASR 1000 Series Routers support almost all the widely used interfaces, and speeds up to OC-192 in all chassis options from the Cisco ASR 1002 Router to the Cisco ASR 1006 Router.

Following is the complete list of SPAs that are supported with Cisco IOS XE Software Release 2.2 at this time:

- 8-port Gigabit Ethernet
- 1-port 10 Gigabit Ethernet
- 2-, 5-, and 10-port Gigabit Ethernet
- 8-port Fast Ethernet
- 8-port T1/E1
- 2- and 4-port T3/E3
- 2- and 4-port OC-3/STM-1 Packet over SONET/SDH (PoS)
- 1-port OC-12/STM-4 PoS
- 2- and 4 –port Channelized T3
- 4-port serial (12-in-1)
- 1-port Channelized STM-1
- 2- and 4-port OC-48 PoS/Resilient Packet Ring (RPR) (PoS mode only)

Further SPA support will come in later software releases.

Infrastructure Security

Cisco ASR 1000 Series Routers are built to enhance the security of the routing infrastructure.

Following are a few platform-related features that provide security to thwart denial-of-service (DoS) and distributed-DoS (DDoS) attacks:

- True isolation of control and data planes: Every transit packet going through the router is forwarded by way of the system data plane; hence control-plane cycles are spent only for traffic that needs route-processor attention.
- Every punt packet (a packet that ends up going to the route processor for processing) has to go through the ESP first, facilitating effective Control Plane Policing (CoPP) performance for all traffic going into the route processor. Because policing in the platform is done in ESP hardware, this process does not result in loading of the route processor.
- Cisco IOS Software Zone-Based Policy Firewall is also supported to further secure the platform and the network users behind it.
- Cisco ASR 1000 Series Routers also allow oversubscription of the platform data plane. You can classify priority traffic to be in the “fast lane” throughout the system (that is, ingress SIP, ESP, and egress SIP) as long as it does not exceed the total system bandwidth (5 Gbps for ESP5 and 10 Gbps for ESP10, etc.).

Sensitive to TCO

TCO accounts for the indirect costs of a network—money spent on system design, installation, administration, and support—along with intangibles such as lost revenue resulting from the failure of mission-critical network functions. Figuring indirect costs allows a company to account for the cost of lost productivity suffered from system crashes, ineffective repairs, and recurring problems.

Cisco ASR 1000 Series Routers exceed the expectations on all parameters relating to TCO. This platform is designed to avoid downtime by using various forms of software and hardware redundancies. In addition, the Cisco ASR 1000 runs on Cisco IOS Software Release 12.2SR, which offers various familiar troubleshooting, maintenance, and instrumentation tools to provide continuous operation. The result is shorter qualification cycles (by using existing scripts and procedures to measure the box performance) and virtual elimination of the retraining requirements for platform configuration and deployment.

Conclusion

The Cisco ASR 1000 Series Routers offer true carrier-class system Internet gateway functions consisting of both routing and forwarding-plane redundant components, high availability, ISSU for Cisco IOS Software with NSF/SSO, and SPA drivers. These routers take advantage of the flexibility and faster services delivery based on the Cisco QuantumFlow Processor starting at 5, 10, and 20 Gbps.

Cisco Services for the Enterprise WAN Edge

Cisco and our certified 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 security and Cisco Unified Communications technologies with bandwidth to support video, collaboration, branch solutions, and growth in alignment with your business goals.

The Cisco lifecycle approach to services defines the requisite activities at each phase of the solution lifecycle. Planning and design expedite solution adoption. Award-winning technical support increases operational efficiency. Optimization improves performance, resiliency, stability, and predictability and prepares your network and teams for change. For more information:

<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.

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website 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. (0809R)