

Cisco ASR 9000 vDDoS Protection

Product Overview

Is your network protected from DDoS attacks? The potential for damage is at an all-time high. The power, frequency, and size and size of these attacks continue to increase at an alarming rate. Results include downtime, potential loss of revenue, decreased network availability, and undue media attention. It is critical to protect your network from these attacks.

Cisco and Arbor Networks have collaborated to bring an industry-leading DDoS solution to this problem. The Cisco ASR 9000 Virtual DDoS Protection solution can create a secure perimeter around your network. And the solution allows you to scale for large and growing service provider and enterprise requirements.

The solution is targeted for deployment at peering points, data center and cloud edge, and enterprise WAN edge to effectively create a secure perimeter around networks. The vDDoS solution runs on the Cisco ASR 9000 Series [Virtualized Services Module](#) (VSM) and is scalable up to 40 Gbps per VSM.

The ASR 9000 vDDoS Protection solution is typically deployed as an “on-demand” solution but can be configured to work in persistent mode. In the “on-demand” mode, only the traffic addressed to the target of the attack is diverted to the vDDoS solution on the VSM; normal traffic is not affected. The vDDoS solution on the VSM module then identifies and blocks malicious attack traffic while allowing legitimate traffic to flow through to its original destination. Business operations continue uninterrupted, even in the midst of a DDoS attack.

The ASR 9000 vDDoS Protection solution is a scalable solution allowing customers to incrementally scale up with just a license or they can install multiple VSMs¹ in a single chassis, incrementally scaling to multiple times the capacity of a single Cisco ASR 9000 Series VSM. This scenario allows the service to scale for large and growing service provider and enterprise requirements.

Evolving DDOS Attacks

DDoS attacks are denial-of-service attacks that take advantage of the compute power of infected devices targeting networks and web servers with a goal of disrupting normal operations costing billions of dollars per year in losses - from lost transactions and customers to damaged reputations and legal liabilities. Today's DDoS attacks are more malicious, destructive, and focused than ever. Launched by disgruntled users, unscrupulous businesses, and extortionists targeting specific sites or competitors, these attacks can easily elude and overwhelm the most common defenses. The ASR 9000 vDDoS Protection solution defends against different types of DDoS attacks, enabling businesses to identify and block malicious traffic without compromising their mission-critical and revenue-bearing operations. Cisco ASR 9000 vDDoS Protection solution uses advanced anomaly-recognition capabilities to dynamically apply integrated source verification and anti-spoofing technologies in conjunction with Intelligence filtering to identify and block individual attack flows while allowing legitimate transactions to pass.

¹ Multiple VSMs per chassis to be supported in a future release

Figure 1 Shows the Cisco ASR 9000 vDDoS Protection positioning, and Table 1 summarizes features and specifications of the solution.

Figure 1. ASR 9000 vDDoS Protection Positioning

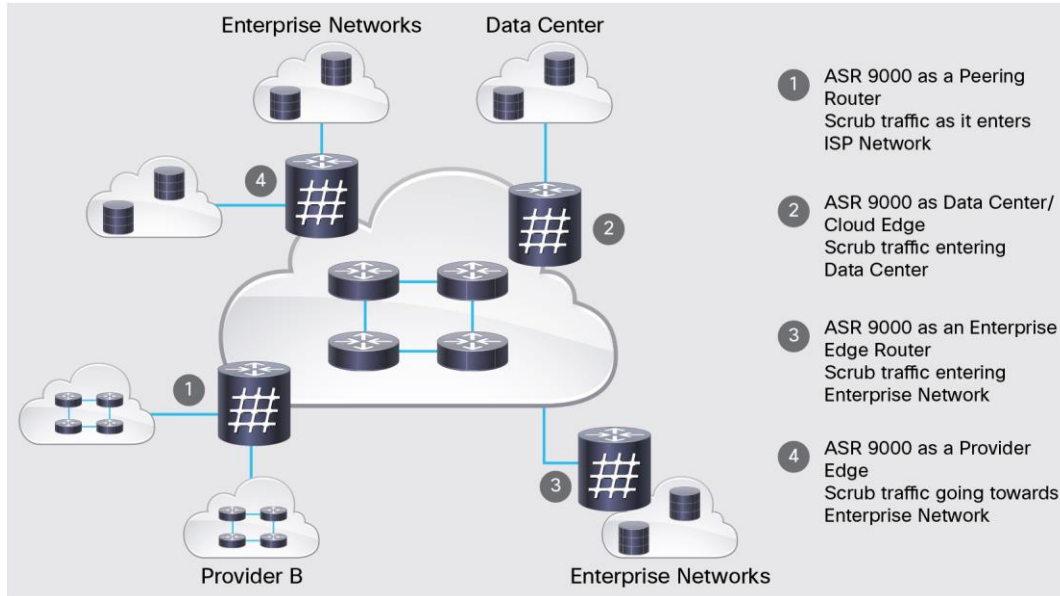


Table 1. ASR 9000 vDDoS Protection Features and Specifications

Feature	Benefit
Throughput	Up to 40 Gbps per VSM
Scalability	Multiple VSMS per system ²
Service management	Service instantiation, activation, and facilitation is performed through the “service-enablement architecture”.
Architecture	Distributed
Tiered licensing	Pay-as-you-grow model has 10-, 20- or 40-Gbps options.
Management	The entire solution is centrally managed through a single console.
Modes supported	Solution can be deployed in “on-demand” or persistent mode.
Block actions	Block actions include source blocking/source suspend, per-packet blocking, and combination of source, header, and rate-based blocking.
Attack protections	Fast-flood attacks (TCP, User Datagram Protocol [UDP], Internet Control Management Protocol [ICMP], Domain Name System [DNS], and Network Time Protocol [NTP] reflection and amplification); fragmentation attacks (Teardrop, Targa3, Jolt2, and Nestatea); TCP stack attacks (SYN, FIN, RST, SYN ACK, URG-PSH, and TCP flags); application attacks (HTTP GET floods, Session Initiation Protocol [SIP] invite floods, DNS attacks, and Secure HTTP [HTTPS] protocol attacks); DNS cache poisoning; vulnerability attacks; resource exhaustion attacks (Slowloris, Pyloris, LOIC, etc.); Flash crowd protection; and IPv4 and IPv6 attacks hidden in Secure Sockets Layer (SSL) encrypted packets
DDoS countermeasures	Blocked list and allowed list, geo location reporting and blocking, zombie blocking, packet content filtering, packet header filtering, Botnet removal (AIF feed), Malformed packet removal (TCP, UDP, DNS, DNSSEC, HTTP, HTTPS, and SIP), multiple antispoofing countermeasures, blended attack protection, Cisco Discovery Network and proxy-aware countermeasures, and rate limiting

² Multiple VSMS per chassis to be supported in a future release

Features and Benefits

Multigigabit Performance

Each VSM is loaded with high-performance processing capabilities to enable attack traffic analysis and cleaning of the traffic, enabling a defense against large-scale DDoS attacks. Multiple VSMs³ can be installed in a single ASR 9000 Series router to provide additional scaling of throughput.

Different Attack Vectors Mitigated

One of the key benefits of the ASR 9000 vDDoS Protection solution is maintaining blocked lists and allowed lists. The allowed list contains authorized hosts, whereas the blocked list contains hosts that have been compromised and whose traffic needs to be blocked. These blocked lists are loaded on the line cards in an ASR 9000 router, effectively increasing the scaling of the solution. This feature can scale 100 Gbps or more with a single VSM in an ASR 9000.

The solution uses complex countermeasures to block application layer exploits. HTTP-specific attacks are detected and mitigated by the solution. DNS services are protected against cache poisoning, resource exhaustion, and amplification attacks. Large reflection attacks such as NTP, DNS, or SNMP are also mitigated by the solution.

Dynamic Diversion

The Cisco ASR 9000 vDDoS Protection solution deploys an “on-demand” scrubbing model. In a typical deployment it is not inserted in the normal data path of the traffic, but can be configured to be inserted in line if the customer so desires; it employs dynamic diversion to automatically redirect only the traffic destined for the destination under attack while the rest of the traffic follows the normal data path. Redirection of the traffic is transparent and can be accomplished using Border Gateway Protocol (BGP) or BGP Flow Spec, etc.

When traffic is scrubbed, all clean or legitimate traffic is then forwarded to the final destination, helping ensure that no critical traffic is lost. By limiting the diverting traffic to only that destined for the target under attack, the vDDoS Protection solution provides optimal resource usage, transparency, and reliability for a scalable solution.

Summary

The Cisco ASR 9000 vDDoS Protection solution is designed for both the service provider and enterprise customers. The solution helps ensure that our customers have uninterrupted business operations, even in the face of the most malicious attacks. Sitting at the edge of the network, the solution provides a secure boundary around the network to safeguard customer network infrastructure and services.

Platform Support and Compatibility

The Cisco ASR 9000 Series vDDoS solution is supported on these Cisco ASR 9000 Series routers:

- Cisco ASR 9904 Router
- Cisco ASR 9006 Router
- Cisco ASR 9010 Router
- Cisco ASR 9912 Router
- Cisco ASR 9922 Router

³ Multiple VSMs will be supported in a future release

Hardware and Software Requirements

The hardware and software requirements for this solution follow:

Hardware:

- Fixed and modular Ethernet line cards (second-generation and later)
- Route Switch Processor 440 (RSP440) or Route Switch Processor 880 (RSP880)
- Cisco ASR 9000 Series Route Processor 1 (RP1) or Route Processor 2 (RP2) for Cisco ASR 9912 and ASR 9922 systems
- Virtualized Services Module (VSM)

Software:

- Cisco IOS® XR Software Release 5.3.0 and later
- Arbor TMS Version 7.0.1 and later

Warranty Information

Warranty information is available on Cisco.com at the [Product Warranties](#) page.

Ordering Information

To place an order, visit the [Cisco Ordering Home Page](#) and use the information provided in Table 2.

Table 2. Ordering Information

Product Name	Part Number
DDoS software licensing for up to 10G of scrubbing	A9K-DDoS-LIC-10G
DDoS software licensing for up to 10G of scrubbing	A9K-DDoS-LIC-10G=
DDoS software licensing for up to 20G of scrubbing	A9k-DDoS-LIC-20G
DDoS software licensing for up to 20G of scrubbing	A9k-DDoS-LIC-20G=
DDoS software licensing for up to 40G of scrubbing	A9k-DDoS-LIC-40G
DDoS software licensing for up to 40G of scrubbing	A9k-DDoS-LIC-40G=
DDoS software upgrade license from 10G to 20G	A9k-DDoS-10U20G=
DDoS software upgrade license from 10G to 40G	A9k-DDoS-10U40G=
DDoS software upgrade license from 20G to 40G	A9k-DDoS-20U40G=

Cisco Services

Through a lifecycle services approach, Cisco delivers comprehensive support to service providers. We help you successfully deploy, operate, and optimize your IP Next-Generation Networks (IP NGNs). Cisco Services for Cisco ASR 9000 Series Aggregation Services Routers provide the services and approach needed to help assure effective deployment. We will help you get the most out of your network investment, with the best possible performance and availability. We deliver our services using leading best practices, tools, processes, and lab environments developed specifically for Cisco ASR 9000 Series deployments and post implementation support. Our Cisco Services team addresses your specific requirements and works to mitigate risk to your existing services, while helping you accelerate time to market for new network services.

For More Information

For more information about the Cisco ASR 9000 Series, visit <http://www.cisco.com/go/asr9000> or contact your local Cisco account representative. Additionally you can visit <http://www.arbornetworks.com/asr9000>.

For more information about Cisco Services, contact your local Cisco account representative or visit: <http://www.cisco.com/go/spservices>.




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.

 Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third party trademarks mentioned 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. (1110R)