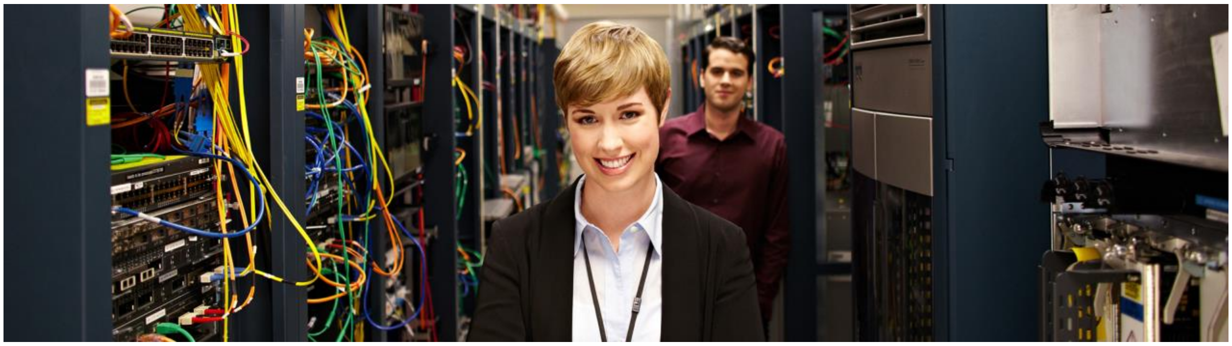


Cisco ASR 9000 vDDoS Protection

BENEFITS

- **Embedded protection:** Make the most of your investment in Cisco ASR 9000 Series routers and Cisco ASR 9000 Series Virtualized Services Modules (VSMs) to embed DDoS protection into your routers. Protect your network availability while reducing the complexity of adding and supporting DDoS protection.
- **Virtualized:** Add DDoS mitigation to Cisco ASR 9000 Series deployments without additional rack space, power, cooling, cabling, and ports, while reducing international importation costs and hassles. You can also deploy Arbor Networks Peakflow for virtualized DDoS detection and analysis.
- **Network edge protection:** Do more to stop DDoS attacks at the network edge and avoid backhauling to regional scrubbing centers.
- **New revenue:** Quickly deliver new virtualized DDoS protection services to your customers.
- **Best in class:** Combine Arbor Networks Threat Management System (TMS) appliances with Cisco ASR 9000 vDDoS Protection deployments for comprehensive DDoS defense that is managed by Arbor Networks Peakflow.

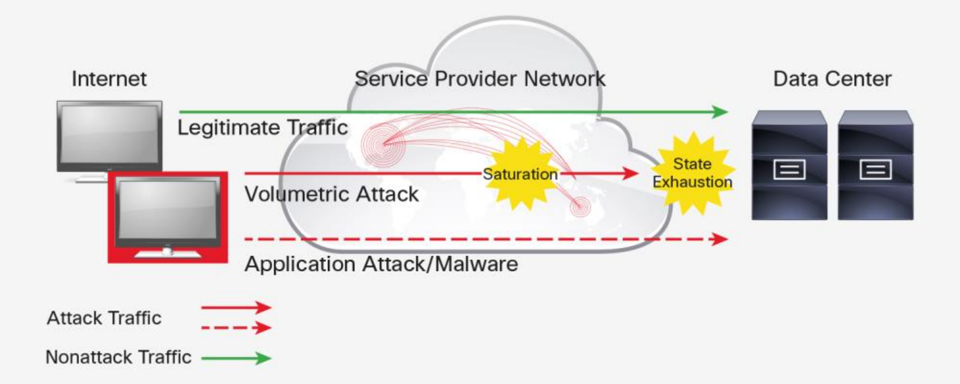
What if your network could detect distributed denial of service (DDoS) attacks and automatically block them? Get empowered to defend your network against volumetric, state exhaustion, and application layer DDoS attacks.

Your network is crucial to your business. If it’s unavailable, your business suffers. When a global botnet launches a DDoS attack against your WAN or LAN, a transit provider, a peer, or one of your customers, your network is in trouble. Links can become saturated with traffic. Network devices, such as routers, and services like domain name system (DNS) can fail. Your customers can lose connectivity, leading to a surge in customer call center volume. To keep your business running, your network must remain available, which means protecting it effectively against DDoS attacks.

Cisco® ASR 9000 virtual DDoS (vDDoS) protection defends your network against DDoS attacks by embedding Arbor Networks DDoS detection and mitigation technology into your Cisco network. The result? You can automatically mitigate all types of DDoS attacks against your network or your customers’ networks. The solution protects your network against different types of DDoS attacks—such as volumetric, state exhaustion, and application layer attacks (Figure 1)—helping to ensure its continued availability. Cisco ASR 9000 vDDoS is completely virtualized, and mitigation is embedded into ASR 9000 Series Routers. So your network is empowered to detect and block

DDoS attack traffic automatically without interfering with the normal flow of traffic. The multitenant solution allows service providers to offer DDoS protection to customers as a service.

Figure 1. Cisco ASR 9000 vDDoS Defends Against Various Types of DDoS Attacks



DDoS Attacks Increase in Size, Frequency, and Complexity

According to Arbor Networks 2014 10th Annual Worldwide Infrastructure Security Report, 73 percent of service provider customers experienced a DDoS attack and 55 percent of service providers experienced a DDoS attack against their infrastructure.

DDoS attacks continue to increase in size and frequency, recently reaching an all-time high of 400 Gbps. These attacks are no longer simple single-vector assaults. They are now typically sophisticated, multiple-vector assaults, or they are part of much larger threat campaigns. Adding to the complexity are new tools available to hackers for launching a dynamic combination of various DDoS attack types, including:

- Volumetric attacks: These attacks target the availability of resources by injecting a large volume of a particular type of traffic or protocol message. The attacks typically target web sites, (particularly online gambling and online games sites), enterprise Internet connections, hosting providers, and cloud providers.
- State exhaustion attacks: These attacks cause the protocol state of targeted resources to overflow and fail. These attacks typically target firewalls, intrusion-prevention systems, web application firewalls, load balancers, and databases.
- Application-layer attacks: These attacks are stealthier in nature and are sometimes referred to as “low and slow.” They target critical applications running in governments, enterprises, and all types of service providers.

How It Works: DDoS Detection and Mitigation

Your network routers send NetFlow to Arbor Networks Peakflow SP collectors running as virtual machines in Cisco Unified Computing System™ (Cisco UCS®). When a DDoS attack is detected, it can be automatically mitigated, or it can be analyzed and manually mitigated. All analysis and management of the DDoS mitigation technologies (Arbor Networks TMS and vDDoS Protection) is performed through Arbor Networks Peakflow SP.

Manual and automatic mitigations are configured by Arbor Networks Peakflow SP. The actual mitigation is performed by vDDoS protection software running on the ASR 9000 Series VSM in a line card slot inside of a Cisco ASR 9000 Series router (Cisco ASR 9006 Router and larger). Both Peakflow and vDDoS protection receive regular updates from the Arbor Networks ATLAS Intelligence Feed (AIF), informing the device about the latest and most relevant DDoS threats from botnets and other sources.

What You Buy

- Cisco ASR 9000 Series router (models: ASR 9006 Router, ASR 9010 Router, ASR 9912 Router, or ASR 9922 Router)
- Cisco ASR 9000 Series VSM
- Cisco ASR 9000 vDDoS Protection
- Arbor Networks Peakflow
- Support for all components
- Installation
- Arbor Networks AIF subscription

Key Capabilities

- DDoS attack detection in as little as one second
- Up to 40 Gbps of mitigation through the ASR 9000 Series VSM
- Up to tens of terabytes per second of blacklisting
- Deployments scale for Tier 1 service provider networks
- Multitenant customer portal

> "By integrating Arbor's proven DDoS mitigation technology into the ASR 9000 router, Cisco is moving aggressively to enable their customers to address the growing size and scale of DDoS attacks. This is a best-of-breed combination."
>
> **— Chris Rodriguez, Senior Industry Analyst, Frost & Sullivan**

Models and Options Available

Cisco ASR 9000 vDDoS Protection: The software is available for mitigation capacities of 10, 20, and 40 Gbps.

Arbor Networks Peakflow: Scales to support any size network, collects NetFlow data, analyzes traffic for DDoS attacks, and provides a portal for customers to log into.

Use Cases

Service provider	• Detect DDoS attacks affecting your network, services, or connectivity. • Mitigate DDoS attacks in your network edge ASR 9000 Series router. • Protect the availability of your network, services, and stateful devices including firewalls, Web Application Firewalls (WAFs), and Intrusion Prevention Systems (IPSs). • Generate revenue from DDoS protection services for your customers.
Internet service provider	• Detect DDoS attacks affecting your network, services, or connectivity. • Mitigate DDoS attacks in your ISP edge ASR 9000 Series router. • Protect the availability of your network, services, and stateful devices, including firewalls, WAFs, and IPSs. • Signal to a cloud DDoS protection service as needed.
Hosting or cloud provider	• Detect ingress and egress DDoS attacks affecting your network, services, or connectivity. • Mitigate DDoS attacks in your ISP edge ASR 9000 Series router. • Protect the availability of your network, services, and stateful devices, including firewalls, WAFs, and IPSs. • Signal upstream to service provider or cloud DDoS protection service as needed.

Mobile network Operator	• Detect and mitigate ingress DDoS attacks towards network infrastructure, services, and devices. • Detect and mitigate egress DDoS attacks originating from mobile devices. • Detect, analyze, and mitigate disruptive traffic coming from misconfigured devices and misbehaving mobile apps.
Over the top provider	• Detect ingress and egress DDoS attacks affecting your network, services, or connectivity. • Mitigate DDoS attacks in your ISP edge ASR 9000 Series router. • Protect the availability of your network, services, and stateful devices including firewalls, WAFs, and IPSs. • Signal upstream to service provider or cloud DDoS protection service as needed.
Enterprise	• Detect DDoS attacks affecting your network, services, or connectivity. • Mitigate DDoS attacks in your ISP edge ASR 9000 Series router. • Protect the availability of your network, services, and stateful devices including firewalls, WAFs, and IPSs. • Signal upstream to service provider or cloud DDoS protection service as needed.
Enterprise data center	• Detect ingress and egress DDoS attacks affecting your network, services, or connectivity. • Mitigate DDoS attacks in your ISP edge ASR 9000 Series router. • Protect the availability of your network, services, and stateful devices including firewalls, WAFs, and IPSs. • Signal upstream to service provider or cloud DDoS protection service as needed.
Government	• Detect DDoS attacks affecting your network, services, or connectivity. • Mitigate DDoS attacks in your ISP edge ASR 9000 Series router. • Protect the availability of your network, services, and stateful devices including firewalls, WAFs, and IPSs. • Signal upstream to service provider or cloud DDoS protection service as needed.

Cisco Capital

Financing to Help You Achieve Your Objectives

Cisco Capital® can help you acquire the technology you need to achieve your objectives and stay competitive. We can help you reduce capital expenditures (CapEx). Accelerate your growth. Optimize your investment dollars and ROI. Cisco Capital financing gives you flexibility in acquiring hardware, software, services, and complementary third-party equipment. And there's just one predictable payment. Cisco Capital is available in more than 100 countries. Learn more.

Data Center Operator Protects Infrastructure and Customers with Arbor Networks and Cisco Capabilities

Challenge

Redundant connectivity allowed a data center operator to handle small, simple DDoS attacks. Then attacks grew larger, more complicated, and more damaging. Volumetric attacks saturated data center connectivity and state exhaustion attacks overran stateful firewalls and IPSs.

Finding budget was challenging, but the service provider decided to deploy Cisco ASR 9000 vDDoS Protection. The solution generated new revenue from DDoS protection services to customers.

Arbor Networks Peakflow detects DDoS attacks in as fast as one second and manages mitigations. Together, Cisco ASR 9000 vDDoS Protection and Arbor Networks TMS—virtualized and embedded in a Cisco ASR 9000 Series router—mitigate DDoS attacks targeting customer networks. Arbor Networks Arbor Cloud provides an extra layer of protection. It helps protect the provider's infrastructure, services, and customers from large volumetric attacks by working to block these attacks in the cloud before they have a chance to saturate Internet connections

Why Cisco?

As an industry leader in networking, Cisco is an ideal partner in building out highly scalable, highly available networks and leveraging knowledge of networks to defend them. DDoS attacks are the greatest security threat to the availability of your network and your customer's networks. Cisco is embedding the industry-leading DDoS detection (Peakflow) and protection technology from Arbor Networks in Cisco ASR 9000 Series routers to help protect your networks at the ingress edge.

> "By adding Arbor's market-leading DDoS mitigation technology to the ASR 9000 router, Cisco is meeting the needs of customers wanting to mitigate DDoS attacks at the network edge. This is a smart move for both companies."
>
> **— Jeff Wilson, Principal Analyst, Infonetics Research**

Next Steps

For more general information about this solution, see the Cisco ASR 9000 vDDoS Protection Solution At-a-Glance. For more information about the details of this solution, see the Cisco ASR 9000 vDDoS Protection Data Sheet. For more information about the technical implementation, scaling, and operation of the Peakflow solution, see the Cisco ASR 9000 vDDoS Protection Solution White Paper.

Additional information can be found at arbornetworks.com/asr9000.

To protect your network against DDoS attacks and deliver DDoS protection services to your customers, contact your Cisco sales representative or Cisco authorized channel partner.

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.**