DDOS SECURE

DDoS Mitigation for your Network and Critical Applications

Product Overview

DDoS Secure defends some of the world's busiest Web servers and critical business applications against volumetric flood and application-layer distributed denial of service (DDoS) attacks. DDoS Secure utilizes advanced heuristic DDoS mitigation technology that dynamically responds to over-loading of the protected resources, automatically providing the full spectrum of DDoS defenses to detect and block attacks. It is used by the world's leading companies and organizations, protecting in excess of $60 billion of revenue. DDoS Secure is today the most comprehensive DDoS mitigation solution available for enterprises and hosting service providers, delivering simple yet effective protection that stops multi-vector DDoS attacks before they can disrupt the availability of your network and critical applications.

Product Description

Juniper Networks® DDoS Secure technology has been ensuring availability of critical business resources for some of the world's busiest e-commerce, financial, and public sector customers for over a decade. During this time, DDoS attacks have evolved from high-bandwidth volumetric attacks that bring down Web servers, to highly sophisticated targeted attacks that threaten availability of critical business applications and resources.

DDoS volumetric flood attacks are still a problem for online businesses, but with the right defense in place, these attacks can be nullified. However, today's new breed of "low and slow" application layer attacks are not as easy to detect, and therefore, are much more difficult to mitigate.

Through an ongoing commitment to innovation with a dedicated focus on solving customers' security needs, Juniper's world-class technology has kept pace with the changing threat landscape in enterprise and service provider networks. By offering a highly effective, fine-grained DDoS mitigation solution, DDoS Secure protects network resources, regardless of which attack vectors are being deployed. DDoS Secure uses a stateful analysis and heuristics approach to DDoS mitigation that provides protection for high volume attacks, as well as advanced "low and slow" application attacks with minimal false positives. The solution delivers fully automated application-layer DDoS protection for Web (HTTP) and secure Web (HTTPS) applications, Domain Name Systems (DNS), and VoIP systems (SIP). DDoS Secure can be deployed as an on-premise hardware appliance or as a virtual machine (VM) in private, public or hybrid cloud environments.

Architecture and Key Components

Heuristic Approach

Traditionally, a DDoS outage occurs when resources are unable to handle the volume of connection requests at a particular point in time. This might be through an induced malicious attack using a Botnet for some financial, ideological, or political motive, or the result of a legitimate "flash-crowd" effect during peak traffic periods. To the end user, there is no real difference—at best they experience degraded response times; at worst, it is a disruption in the resource's availability resulting in an outage with serious business impact.

Adding more horsepower to the server or increasing bandwidth connectivity can provide some insurance against a volumetric DDoS attack, but they are ultimately in-effective against today's new breed of sophisticated DDoS threats. Simply throttling all traffic or blacklisting particular groups of IP addresses is also not a lasting solution, particularly as these measures can impact legitimate users.

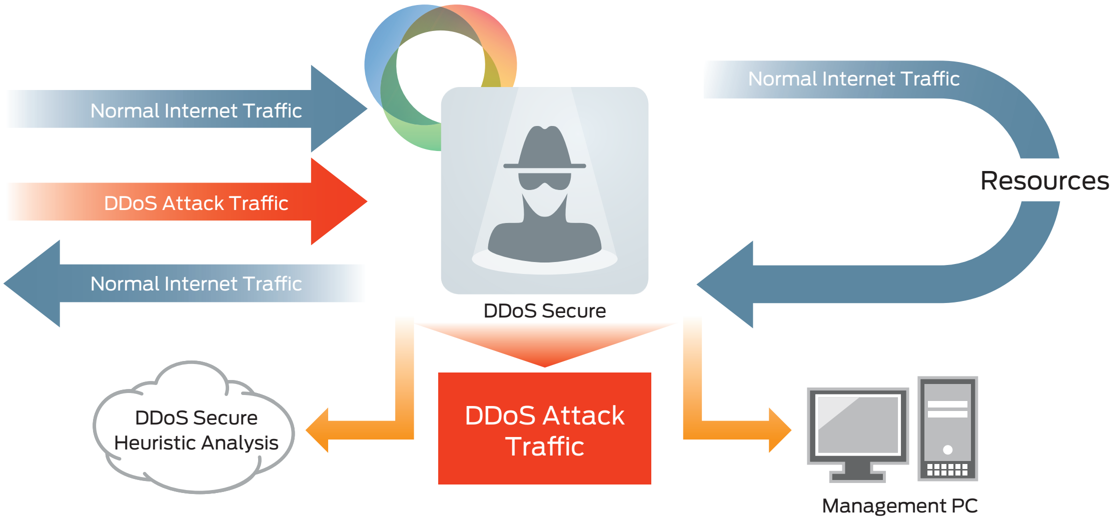
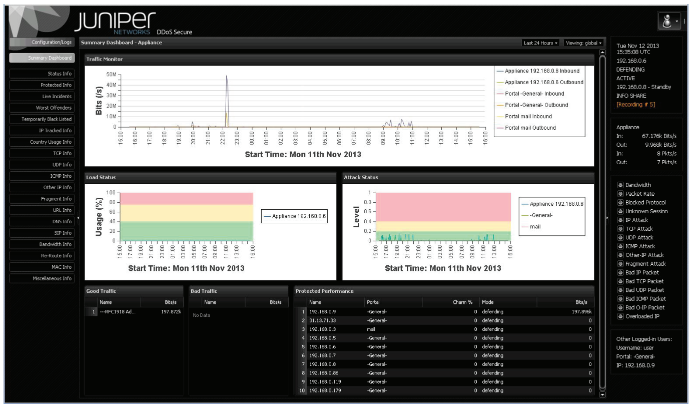


Figure 1: DDoS Secure heuristic mitigation in action. Normal Internet traffic flows through the DDoS Secure device, while the software analyses the type, origin, flow, data rate, sequencing, style and protocol being utilized by all inbound and outbound traffic. The analysis is heuristic in nature and adjusts over time but is applied in real time with minimal latency.

DDoS Secure software is different. Its innovative heuristic technology continually monitors and logs all inbound and outbound network traffic. Using its unique CHARM algorithm DDoS Secure learns which clients pose a risk through their use of available resources, and then intelligently responds in real time by disrupting an attack as soon as performance of critical resources begins to degrade.

This heuristic and granular approach to DDoS mitigation guarantees availability for legitimate users while blocking bad traffic, even under the most extreme attack conditions.



Tue Nov 12 2013
15:35:08 UTC
192.168.0.6
DEFENDING
ACTIVE
192.168.0.8 - Standby
INFO SHARE
[Recording # 5]

Appliance

In:	67.176k Bits/s
Out:	9.968k Bits/s
In:	8 Pkts/s
Out:	7 Pkts/s

Good Traffic

	Name	Bits/s
1	---RFC1918 Ad...	197.872k

Bad Traffic

	Name	Bits/s

No Data

Protected Performance

	Name	Portal	Charm %	Mode	Bits/s
1	192.168.0.9	-General-	0	defending	197.896k
2	31.13.71.33	-General-	0	defending	0
3	192.168.0.3	mail	0	defending	0
4	192.168.0.5	-General-	0	defending	0
5	192.168.0.6	-General-	0	defending	0
6	192.168.0.7	-General-	0	defending	0
7	192.168.0.8	-General-	0	defending	0
8	192.168.0.86	-General-	0	defending	0
9	192.168.0.119	-General-	0	defending	0
10	192.168.0.179	-General-	0	defending	0

Other Logged-in Users:
Username: user
Portal: -General-
IP: 192.168.0.9

Figure 2: The DDoS Secure summary dashboard displays inbound and outbound traffic, attack and load status, good and bad traffic as well as performance of the protected resource.

Key Features and Benefits

- Bi-directional traffic analysis and inspection
- Dynamic and self-learning thresholds and critical resource limits
- Effective against the latest application layer and stealth attack vectors
- Ultra-low latency solution
- Fully IPv6 compliant
- Plug-and-play, simple to install, configure, and operate
- Fail-safe and high-availability options
- Protection against DNS amplification attacks
- SSL inspection enables protection of HTTP and HTTPS applications
- STRM integration allows visibility into incident and status events, logging and reporting
- Fully automated for the fastest response and the lowest cost of ownership

Ease of Deployment

DDoS Secure operates as a Layer 2 transparent bridge positioned inline between the Internet and the core network infrastructure, making it easy to set up and begin defending critical resources within 10 minutes of powering on, without requiring any changes to the network architecture.

DDoS Secure can be deployed as a 1U appliance or virtual instance. It supports HA active/standby pairs and active/active pairs for asymmetric routing. These low latency (sub-millisecond) advanced DDoS Secure solutions are today protecting some of the world's most demanding customers 24 x 7, 365 days a year.

Using advanced dynamic distributed threat intelligence (DDTI) techniques, DDoS Secure also ensures that when a threat is detected at one gateway, within seconds all the other DDoS Secure appliances in the logical network are updated with the latest information needed to protect critical resources.

Virtualization

For maximum flexibility of deployment, DDoS Secure is also available to operate in a range of virtualized environments, including VMware and KVM-based systems. Virtualization offers larger enterprises the ability to rapidly set up and configure a global DDoS defense shield using spare server capacity in their regional data centers.

Virtualization also provides Internet service providers with the ability to easily roll out DDoS mitigation as an additional managed service for customers by leveraging their existing virtual infrastructure.

24/7, 365-Day Resource Optimization

In addition to its unrivaled DDoS mitigation capabilities, DDoS Secure also incorporates a range of network performance monitoring and analysis tools to give data center managers fine-grained control over the network resources.

DDoS Secure's fully stateful inspection engine analyzes every incoming and outgoing packet. By measuring the physical and application response times, the DDoS Secure appliance automatically adjusts the flow rate to ensure optimal performance of the protected resources. Key performance indicators are fed into the Resource Optimization Console, providing the customer with a fast and powerful set of management tools to highlight bottlenecks and manually fine-tune the response times of all DDoS Secure protected resources.

Specifications

Hardware Platform

Features	1200-C	1200-SR / 1200-LR
Performance		
Throughput each direction	1Gbps	10Gbps (per system; clustering supports up to 160Gbps throughput capacity)
IPs protected	64,000	64,000
Tracked IPs (IPv4/IPv6)	32 million	32 million
Concurrent TCP sessions	4 million	4 million
Setup session rate	750 kcps	750 kcps
Connectivity		
Network interface	1G copper	10G fiber SR/LR
Physical Specification		
Height	1RU	1RU
Width	48.2 cm	48.2 cm
Depth	77.2 cm	77.2 cm
Weight	39.0 lb	39.0 lb
Number of blades	N/A	N/A
Intel Xeon CPU	8 Core	8 Core
RAM	32 GB	32 GB

Ordering Information

What to Buy

This product adheres to the Juniper Software Advantage pricing model, thus please be advised of the following items that constitute an order:

- Select a software license based on the throughput required. The license is either subscription (fixed term) or perpetual (unlimited term).
  - A subscription software license includes Juniper Care Software Advantage, entitling you to software updates and upgrades, 24x7 remote technical support, and online support.
  - A perpetual software license excludes Juniper Care Software Advantage; the latter must be purchased.
- If your order includes a hardware product/platform, select a hardware license based on your networking, connectivity, and/or security requirements (e.g., interface options, I/O, services). You may need to purchase additional licenses in support of the base hardware license (e.g., power cables, network interface cards).
- If this is a virtual appliance/software product, you would not buy any hardware license from Juniper, but, instead, procure the hardware elsewhere. For information on supported hypervisor(s) and virtual machine (VM) requirements, please refer to the technical documentation for this product on our Website (**www. juniper.net**) under the support section.

Juniper Networks products are sold directly as well as through Juniper partners and resellers. For more information on the Juniper Software Advantage business model, please visit **www.juniper.net/us/en/products-services/security/**

For information on how to buy, please visit: **www.juniper.net/us/ en/how-to-buy**

About Juniper Networks

Juniper Networks is in the business of network innovation. From devices to data centers, from consumers to cloud providers, Juniper Networks delivers the software, silicon and systems that transform the experience and economics of networking. The company serves customers and partners worldwide. Additional information can be found at **www.juniper.net**.

Corporate and Sales Headquarters

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, CA 94089 USA
Phone: 888.JUNIPER (888.586.4737)
or +1.408.745.2000
Fax: +1.408.745.2100
www.juniper.net

APAC and EMEA Headquarters

Juniper Networks International B.V.
Boeing Avenue 240
1119 PZ Schiphol-Rijk
Amsterdam, The Netherlands
Phone: +31.0.207.125.700
Fax: +31.0.207.125.701

To purchase Juniper Networks solutions, please contact your Juniper Networks representative at +1-866-298-6428 or authorized reseller.

1000426-002-EN Nov 2013

Printed on recycled paper