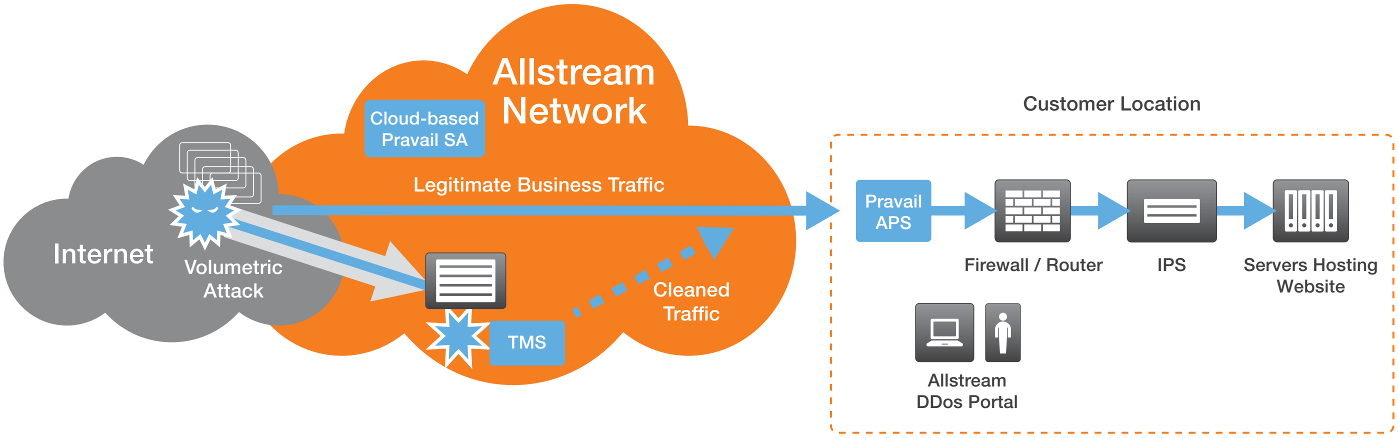
DDoS Protection Service Overview

Internet-borne Distributed Denial of Service (DDoS) attacks represent a major threat for business organizations irrespective of their size or the industry in which they operate. A successful attack can paralyze operations, trigger significant financial losses and damage business reputations and brands that took a lot of effort to build.

As attacks are growing in frequency and sophistication, businesses are searching for solutions that effectively neutralize the DDoS threat while allowing their networks to continue to operate without performance impairments.

Allstream DDoS Protection with Pravail APS and cloud-based Pravail SA



Allstream DDoS Protection Services

Allstream DDoS protection offers businesses an effective solution that stops DDoS attacks by using network based intelligence to monitor traffic, detect anomalies and to remove potential threats before they can impact your network.

Based on industry-leading Arbor “Peakflow SP” technology, Allstream DDoS protection provides advanced traffic-scrubbing and redirection capabilities that act to defend networks against targeted attacks and maintain the uptime and availability of business critical applications.

For a complete protection solution, Allstream’s network based DDoS service can be supplemented by implementing additional products and services including:

- A customer premise based Arbor “Pravail (APS)” unit that will stop DDoS attacks that exploit application layer complexities in order to target and disable your online business.
- A cloud-based and/or customer-premise-based Arbor “Pravail Security Analytics (Pravail SA)” collector that provides an unprecedented and detailed view of attacks in network traffic based on Big Data fueled by world-class research.

Advantages of Allstream DDoS protection

- Features a mitigation architecture called “diversion/injection” that directs suspicious data streams to one of the Threat Management Systems (TMS) located within the Allstream network where the malicious traffic from that stream is discarded, while the legitimate traffic is forwarded to its intended destination. This approach, also called “surgical mitigation”, helps ensure the uninterrupted flow of legitimate network traffic and is superior to other solutions that, in order to stop a DDoS attack, block the entire data stream while impacting useful traffic in the process. Allstream’s DDoS protection with the diversion/injection architecture is illustrated on the previous page.

- Harmful DDoS traffic can affect hosts, subnets and devices that share the same network with the intended victim of the attack. In contrast with other DDoS countermeasures, Allstream DDoS protection service is able to isolate, reroute and scrub the traffic destined to the attackers’ target while allowing the other elements of the network to function unimpeded.

- Unlike firewalls and Intrusion Prevention Systems (IPS), which are normally in-line stateful devices and are in danger to be overwhelmed and disabled by malicious traffic, Allstream's DDoS protection continuously monitors/analyzes traffic flows and can stop an attack long before it reaches the customer’s network.

When DDoS protection includes both Allstream’s network based protection service and a Pravail APS appliance installed on the premises, the customer network is protected against both volumetric attacks that try to overwhelm it and application layer attacks that generate lower traffic levels but are just as damaging.

Key Features and benefits

Effective, intelligent protection against DDoS attacks
Protects the overall performance of the network and the critical applications running on it

Rapid deployment through self-learning
The system quickly learns the normal traffic patterns and is able to alert on anomalous traffic and mitigate against malicious traffic

Surgical mitigation
Automatically removes the attack traffic without interrupting the flow of legitimate business traffic. Mitigation areas include:

- Blocking known malicious hosts through use of behavioural algorithms combined with optional black lists and white lists

- Removing malicious traffic addressed to the attack’s intended target while leaving all other traffic to continue its normal path

- Routing traffic addressed to the victim via scrubbing centres leaving all other traffic unaffected

- Identifying and blocking traffic originating from zombie army (botnets) computers

Choice of mitigation methods
Allows customers to choose among automatic mitigation of attacks based on pre-established criteria, manual real-time mitigation or a combination of both

Application layer DDoS protection
In addition to defending the network against lower layers DDoS attacks, a Pravail APS unit installed on the premises will defend against DDoS attacks in real time that target the application layer (including both TCP and UDP supported applications). More specifically, it will defend against attacks targeting protocols like HTTP, SSL, ICMP, VoIP (SIP), DNS and SMTP. To perform this task, the Pravail APS unit uses both behaviour algorithms and the most current intelligence about DDoS attacks signatures. That intelligence is provided through a feed from ATLAS (Arbor Active Threat Level Analysis System), a global network of probes that continuously gather DDoS attack information. Being a stateless device, the Pravail APS unit is normally placed in front of firewall or IPS devices. Here is a summary of its most important benefits :

- Provides onsite visibility and answers the immediate question of “are we under attack?”

- HTTPS/SSL protection without decryption of network traffic

- Full Internet pipe DDoS protection up to the circuit bandwidth

- Protection against low bandwidth and connection exhaustion types of attack

- In-line / “always on” 7x24x365 protection for networks that connect to the Internet through multiple ISPs

- Complements and enhances cloud based DDoS protection services

Protection based on best security analytics

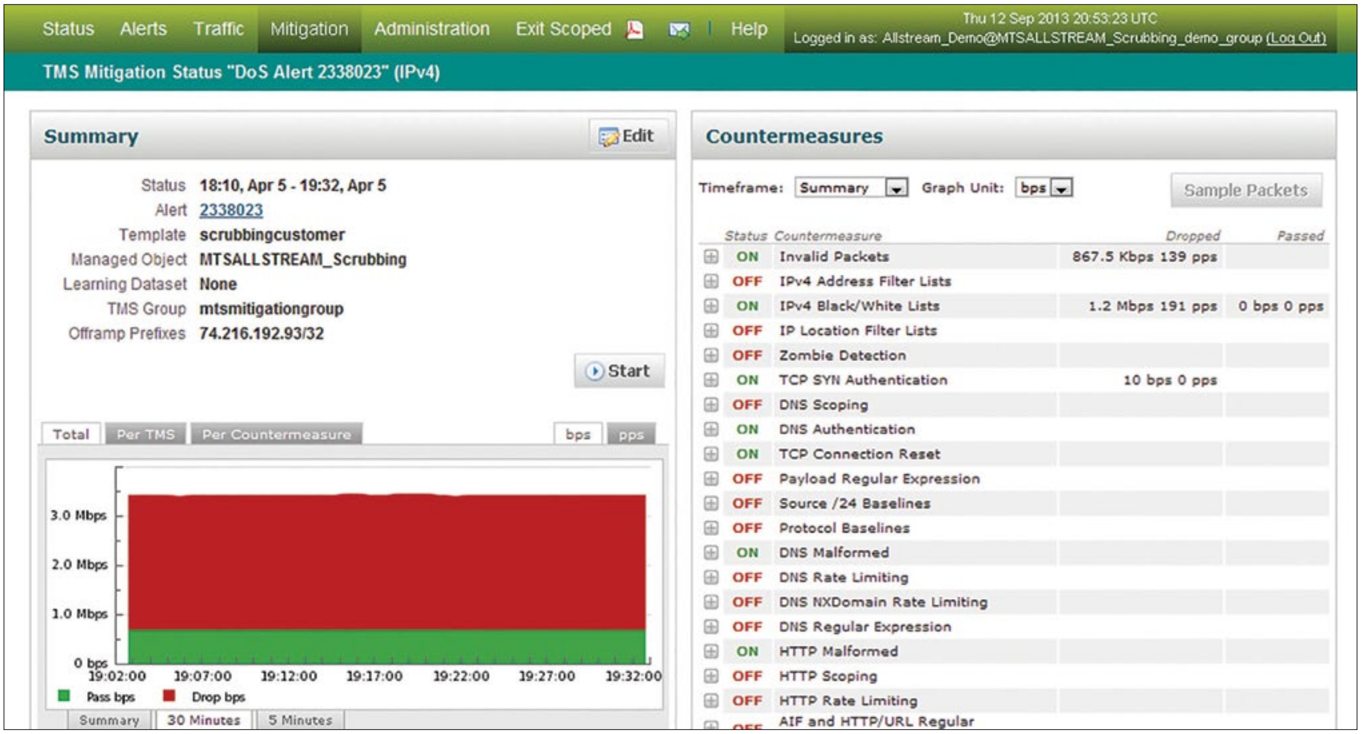
The use of a customer or cloud based Pravail Security Analytics (Pravail SA) unit further enhances a network's DDoS protection by offering an exceptionally detailed view of previously captured attacks and network traffic. The benefits of Pravail SA include:

- Ability to explore and better understand attacks across the network in either real time or historical fashion
- Isolate and study attacks based on specific criteria: duration, severity, originating host, location country, etc.
- Use of established benchmark to determine whether a network is overly targeted
- Ability to reveal previously undetected attacks through thorough search of historical traffic
- Updates trigger automated re-examination of captured data to uncover potential or active threats
- Unmatched flexibility allows customers to interact with their data by zooming in and out from years to minutes or move forward and backward in time as required by current security needs

Real time mitigation tools

Allstream DDoS protection portal offers extensive flexibility in tailoring mitigation filters and activities to the needs of an organization at a given time. Portal functionality includes:

- Alert detail information: severity indicators (high, medium, low), anomaly type (misuse or bandwidth), TCP traffic indicators, list of protocols affected (ICMP, UDP, TCP, etc.), list of affected devices, list of current blocked attackers, source IP addresses, etc.
- Traffic reports: statistics, graphs, ability to drill down into specific events, real time information about inbound and outbound traffic trends for the protected IP space.
- Mitigation tools: filter set up, set up of zombie definitions, focus on particular applications or DNS service, ability to change parameters in real time.
- Administrative features: comprehensive set of security, management and reporting capabilities.
- Canadian-based: Allstream TMS systems are located within scrubbing centres in Toronto and Calgary so customers' data never leaves Canada once it has reached Allstream's network.
- Real time information and trends of the scrubbing process throughout an attack.
- A typical Allstream portal screen during the mitigation of a DDoS attack is shown below.



Thu 12 Sep 2013 20:53:23 UTC
Logged in as: Allstream_Demo@MTSALLSTREAM_Scrubbing_demo_group (Log Out)

TMS Mitigation Status "DoS Alert 2338023" (IPv4)

Summary

Status	18:10, Apr 5 - 19:32, Apr 5
Alert	2338023
Template	scrubbingcustomer
Managed Object	MTSALLSTREAM_Scrubbing
Learning Dataset	None
TMS Group	mtsmitigationgroup
Offramp Prefixes	74.216.192.93/32

Countermeasures

Timeframe: Summary Graph Unit: bps

Status	Countermeasure	Dropped	Passed
ON	Invalid Packets	867.5 Kbps 139 pps	
OFF	IPv4 Address Filter Lists		
ON	IPv4 Black/White Lists	1.2 Mbps 191 pps	0 bps 0 pps
OFF	IP Location Filter Lists		
OFF	Zombie Detection		
ON	TCP SYN Authentication	10 bps 0 pps	
OFF	DNS Scoping		
ON	DNS Authentication		
ON	TCP Connection Reset		
OFF	Payload Regular Expression		
OFF	Source /24 Baselines		
OFF	Protocol Baselines		
ON	DNS Malformed		
OFF	DNS Rate Limiting		
OFF	DNS NXDomain Rate Limiting		
OFF	DNS Regular Expression		
ON	HTTP Malformed		
OFF	HTTP Scoping		
OFF	HTTP Rate Limiting		
OFF	AIF and HTTP/URL Regular		

Managed DDoS Portal Service

Allstream offers a Managed DDoS Portal service that better serves customers who prefer monitoring, analysis and mitigation of their DDoS portal to be done externally while they focus their internal IT resources on the strategic needs of their organization.

Managed DDoS Portal service includes:

- **Monitoring and Support**
  Allstream will monitor all events from the Customer's DDoS portal and will flag all alerts and critical event notifications generated by the portal. Monitoring and support will be available on a 24/7 basis with a guaranteed 30 minutes response time from a live Allstream network security specialist.

- **Mitigation**
  In case of attack, affected incoming traffic will be redirected to a special facility where it will be "scrubbed" by having harmful streams of data removed and legitimate data redirected back to the customer. Outgoing traffic will continue to flow through the normal path.

  Allstream will keep the customer informed of the mitigation action that takes place and of possible Internet access disruptions. Depending on the severity of the attack and its impact on the organization, communications may include email, phone notifications and live conference calls with Allstream specialists.

  Allstream will also retain for 12 months the history of mitigation incidents and all the high-level alerts associated with the customer's network.

- **Reports**
  Customers can log into their account on the Allstream DDoS portal and view comprehensive reports characterizing data traffic into the organization's network. The information on the reports can be accessed in detailed or summarized form and can be focused on particular applications, data sources or protocols.

- **Service Provisioning**
  Allstream will install and activate the DDoS service and will gradually hand-off control of the service to our Security Operations Centre (SOC). During the hand-off period Allstream will work with the customer to create a comprehensive risk assessment and to fine tune the parameters of the service in accordance to their specific needs.

- **Updates and maintenance**
  On an ongoing basis, Allstream will ensure the customer's DDoS service is up-to-date by installing updates and patches as required. When necessary, customers will be notified of the details of the updates and the timing of their introduction.

Why Allstream?

Allstream is the only national communications provider working exclusively with business customers. Our focus is helping you simplify IT operations to improve productivity, maximize performance and manage costs. Allstream DDoS protection service enables businesses to defend their assets against malicious attacks and helps them maximize the performance of their IP networks. Our IP solutions are delivered on a fully managed, fully secure national network and backed by our industry-leading commitment to customer service: The Allstream Service Guarantee.

We can help you compete more profitably by converging voice and data over a single, reliable, end-to-end infrastructure that delivers exceptional quality of service between metropolitan centres.

eIP

For more information,
please visit allstream.com

allstream®