NoviFlow

NoviAccelerator

Effective and Affordable Multi-Terabit Volumetric DDoS and TCP State Exhaustion Mitigation for CSP Networks

Highlights

Mitigates Tbps of volumetric DDoS and TCP state exhaustion attacks and with microsecond port-to-port latency

Switch-based mitigation and congestion control with Intrusion Detection System (IDS)

Scales with very large attacks by transitioning portions of the mitigation to destination IP metering with DSCP remark.

Provides congestion control and load balancing in the switch for in-depth resilience and independent scaling of the IDS

Minimizes false positives, enhancing the overall accuracy of threat detection

Enables the IDS to be managed independently of the network forwarding, reducing network complexity and enhancing security

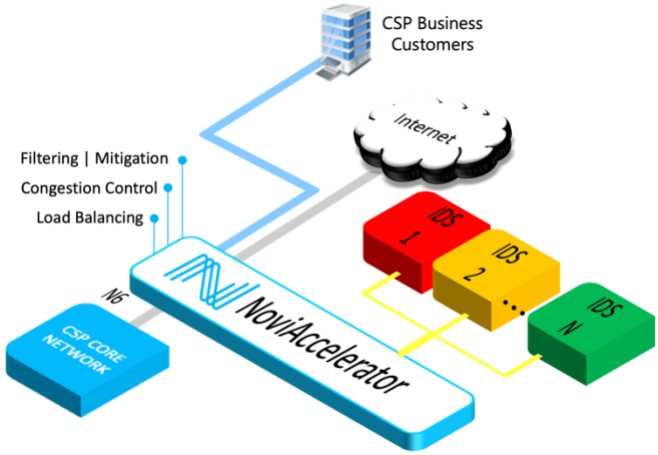
Delivers Multi-Tbps performance at significantly lower costs compared to traditional solutions.

NoviAccelerator unites multi-Tbps switch-based mitigation and congestion control with x86 based Intrusion Detection System (IDS) to economically detect and mitigate Volumetric DDoS and TCP state exhaustion attacks.

Volumetric DDoS attacks pose a significant risk to businesses worldwide. Communications Service Providers (CSPs) are prime targets for these attacks, facing consequences such as software/hardware costs, revenue reduction, loss of consumer trust, customer data theft, financial theft, and intellectual property loss. The average cost per DDoS incident has risen as high as half a million dollars for large enterprises.

As CSPs provide ever-higher access speeds they face a challenge with fixed wireless access, where they lack control over WIFI-connected devices. A critical problem they encounter is the detection and mitigation of DDoS attacks on corporate customers originating from infected devices (BOTs) within their own subscriber base.

NoviAccelerator with IDS Solution protects the CSP from becoming the source of DDoS attacks on their corporate customers. NoviAccelerator offloads the mitigation function for Volumetric DDoS and TCP state exhaustion attacks to a multi-Tbps forwarding plane and reduces cybersecurity costs by freeing up the x86 virtual processing capacity of the IDS.



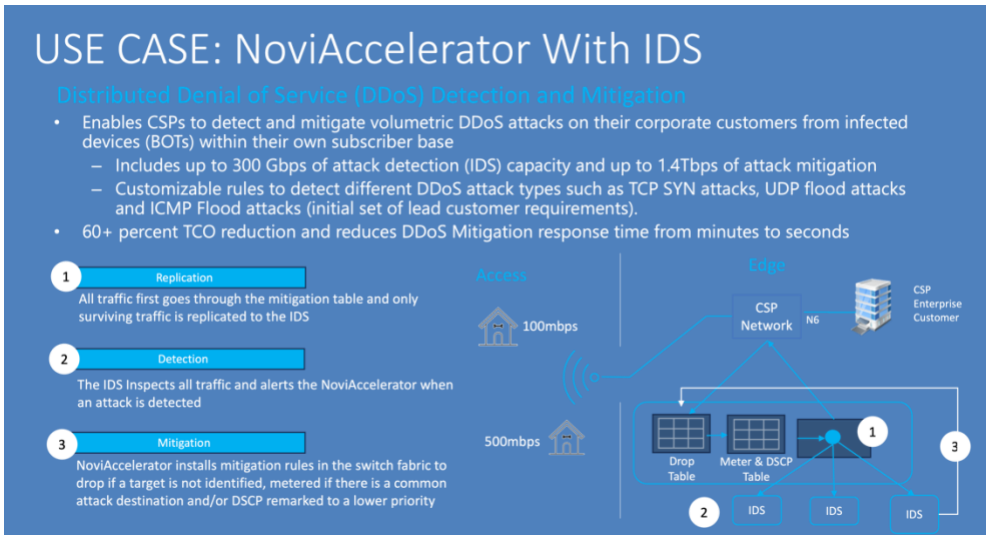
NoviAccelerator scales with very large attacks by adding metering with DSCP remark functionality. The algorithm implements metering for the most attacked services (destination IPs). The DSCP remark enables the CSP's downstream network to make smart decisions on which packets to drop if congestion become high. NoviAccelerator also implements congestion control to the IDS, further enhancing network resilience and business continuity in the face of increasingly sophisticated cyber threats.

NoviAccelerator is an economical and comprehensive solution that provides unparalleled protection against volumetric DDoS attacks at significantly reduced costs thanks to Open-Source software and Commercial Off-The-Shelf (COTS) hardware.

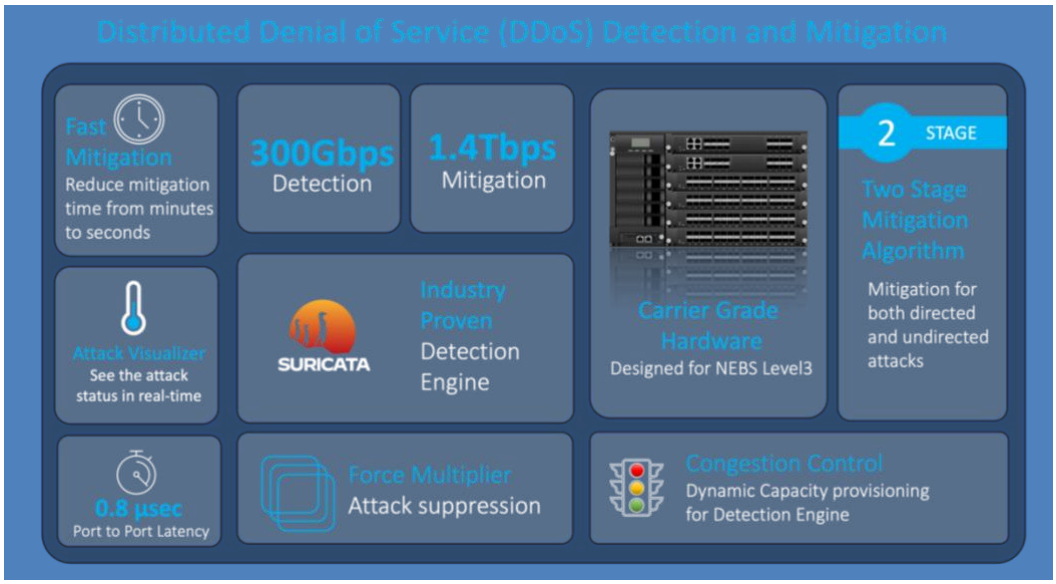
Use case: N6 Filter

Problem:
CSPs need to detect and mitigate certain DDoS attacks on their corporate customers from infected devices (BOTs) within the CSPs subscriber base.

Solution:
NoviAccelerator with IDS Solution detects and mitigate UDP flood, TCP SYN flood and ICMP flood DDoS attacks from the CSP's own subscribers.



NoviAccelerator Characteristics



NoviFlow Operations Monitoring Suite

NoviAnalytics monitors an instance of *NoviAccelerator*, allowing operators to live-monitor over 75 different hardware sensors, OS log files and application messages to fully understand the operational health and performance of the *NoviAccelerator*. *NoviDashboard* provides a single pane of glass to monitor an entire fleet of *NoviAccelerator* instances and flags any fault or warning across all *NoviAccelerator* in the monitored fleet.

Together these make it possible to troubleshoot problems, take preventative measures and ensure a higher level of uptime. Information updates are real-time indicators of the overall health of the platform. If a sensor reports a fault or out of tolerance, live historical data with the key information needed for troubleshooting is available with two clicks.

Features	Benefits
Multi-Tbps of volumetric DDoS and TCP state exhaustion attacks and with microsecond port-to-port latency	• Detects and mitigates common large volumetric DDoS and TCP state exhaustion attacks • Customizable rules to detect different DDoS attack types such as TCP SYN attacks, UDP flood attacks and ICMP Flood attacks (these make up over 80% of DDoS attack packet volume). • It greatly reduces the cost-per-bit-inspected via intelligent filtering • Supports over 500,000 IPv4/IPv6 mitigation drop rules • Sub-micro-second In-line mitigation of metering/remark • Up to 300 Gbps of attack detection (IDS) capacity and up to 1.4Tbps of attack mitigation
Scales to handle very large volumetric DDoS attacks with destination service (dstIP) metering and DSCP remark	• Protects most attacked services (destination IPs) from being compromised in very large attacks • Provides escalation policy when the limit of IPv4/IPv6 mitigation drops is reached • Provides information, DSCP remark, to CSP's downstream network that the packet is headed for a device under attack and is a good candidate for drop if there congestion • Opens space in mitigation table for drop rules to other devices
Provides congestion control and load balancing in the switch for improved security, in-depth resilience and independent scaling of IDS	• Reduces DDoS Mitigation response time from minutes to seconds • Congestion Control protects IDS from being overrun thus improving network stability and improving IDS performance • Minimizes the attack surface by implementing only the functions needed by the CSP for the solution • Invisible to external attackers
Reduces IDS costs by minimizing false positives, enhancing the overall accuracy of threat detection, and enabling CSPs to decide how much to invest in the IDS inspection capacity	• Maximizes value/performance of IDS services: Active/standby redundant services can be deployed at full utilization – doubling (or more) payload processing with existing IDS investments • Enables the user to decide how much to invest in the IDS inspection capacity
Pre-integrated solution leverages Open-Source software and COTS hardware to deliver Tbps performance at significantly lower costs compared to traditional solutions	• Disaggregated solution that runs on COTS hardware • Detects and mitigates common large volumetric DDoS and TCP state exhaustion attacks at a significantly lower cost compared to traditional solutions • Up to 60+ percent TCO reduction

Ordering Information

NoviAccelerator on Lanner HTCA-6600 (Tofino32D)			
NoviFlow Direct	Perpetual license	802-000-001	NoviAccelerator Perpetual RTU Software license for Barefoot Tofino-32D-based switches (per switch)
		200-100-116	NoviWare perpetual license for Lanner HTCA-6600 switch blade (Tofino-32D)
		3rd Party Provided	Lanner HTCA 6600
	Annual Support (1, 2, 3, 5 years available)	513-100-001	NoviAccelerator for Tofino-32D switch Software Support Services - 1 year per switch
		501-100-116	NoviWare for Lanner HTCA switch blade (Tofino-32D) Software Support and Upgrade Service - 1 year (per switch)
		803-000-001	Suricata software distribution (zero cost)
		514-100-001	Suricata per compute blade SSU 1 year

NoviAnalytics for NoviAccelerator Ordering Information

NoviAnalytics for NoviAccelerator on Lanner HTCA-6600 (Tofino32D)			
NoviFlow Direct	Perpetual license	800-005-200	NoviAnalytics for NoviAccelerator on Tofino32D switch Perpetual Software Right to Use License Fee
	Annual Support (1, 2, 3, 5 years available)	515-100-001	NoviAnalytics for NoviAccelerator on Tofino32D switch Software Support Services - 1 year per switch

NoviDashboard Ordering Information

NoviDashboard (Fleet monitoring)			
NoviFlow Direct	Perpetual license	800-005-900	NoviDashboard software option Perpetual Software RTU License Fee
	Annual Support	800-005-901	NoviDashboard software option subscription fee per year per connected NoviAnalytics instance

Platform Requirements

NoviFlow Software	CPU	Memory	Storage	Software
NoviAccelerator	4 core CPU @ 2.1 GHz	4GB RAM	50 GB	Ubuntu 20.04, Docker v19.03 or later, Docker-composer v 1.24
NoviAnalytics for NoviAccelerator	Min. 4 core CPU @ 2.1 GHz (8 core recom.)	Min. 4GB RAM (12GB recom.)	Min. 50 GB (100GB recom.)	Ubuntu 20.04, Docker v19.03 or later, Docker-composer v 1.24