Arbor Threat Mitigation System (TMS)

Proven, Comprehensive Threat Protection and Service Enablement

KEY FEATURES & BENEFITS

Surgical Mitigation

Automatically remove only the attack traffic without interrupting the flow of non-attack business traffic.

Full Portfolio of Mitigation Platforms and Capacities

Choose from a variety of mitigation platforms and capacities including: 2U appliances (500 Mbps–400 Gbps), 6U chassis (10– 100 Gbps); virtualized in Cisco ASR 9000 Router (10– 60 Gbps) and KVM & VMware hypervisor (1-40 Gbps).

Unified Command and Control of Eight Tbps of Mitigation

Scale DDoS defenses to an unprecedented level. Deploy up to eight terabits of aggregate, centrally-managed mitigation capacity per deployment.

Managed Services Enabler

Meet rapidly growing demand for DDoS protection services. Use Arbor TMS to deliver profitable in-cloud DDoS protection services.

Comprehensive List of Attack Countermeasures

Protect your infrastructure and/or your customers from the largest and most complex volumetric, TCP-state exhaustion and application-layer DDoS attacks.

Flexible Deployment

Deploy application-layer intelligence, threat detection and surgical mitigation in different portions of your network for infrastructure protection and more profitable managed DDoS protection services.

Internet Service Providers (ISPs), Cloud Providers and Enterprises face a common problem. Distributed Denial of Service (DDoS) attacks are a major risk to service availability. The power, sophistication and frequency of DDoS attacks continue to increase. Data center operators and network providers need a defense that is effective, cost-efficient and easily managed. Arbor Threat Mitigation System (TMS) is the acknowledged leader in DDoS protection. More Service Providers, Cloud Providers and large Enterprises use Arbor TMS for DDoS mitigation than any other solution.

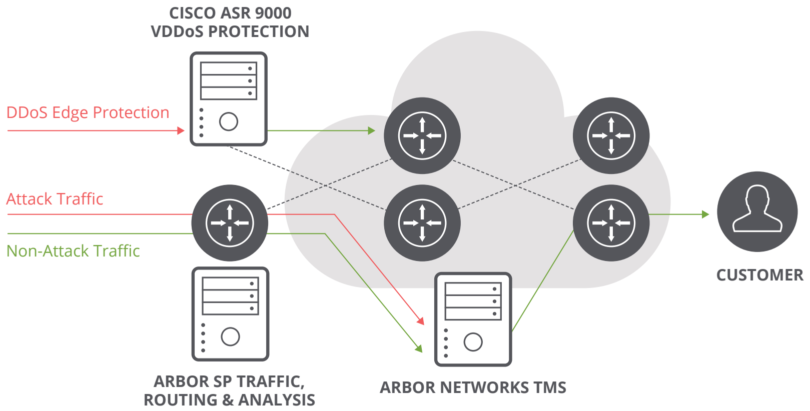
Orchestration and Automation for DDoS Protection

The Arbor solution integrates network-wide intelligence and anomaly detection with carrier-class threat management to help identify and stop volumetric, TCP state exhaustion and application-layer DDoS attacks.

Arbor TMS network appliances provide the vital, traffic-scrubbing component of the Arbor solution. Arbor TMS can be deployed inline to provide an automated ‘always on’ solution. Unlike other products, it also supports a mitigation architecture called “diversion/reinjection.” In this mode, only the traffic stream carrying the DDoS attack is redirected to Arbor TMS through routing updates issued by the Arbor solution. Arbor TMS removes only the malicious traffic from that stream and forwards the legitimate traffic to its intended destination.

This is highly advantageous for Service Providers, large Enterprises and large Hosting/Cloud providers. It enables a single, centrally located Arbor TMS to protect multiple links and multiple data centers. It results in much more efficient use of mitigation and fully non-intrusive security. Inline devices must inspect all traffic all the time on the links they monitor. Arbor TMS only needs to inspect traffic that is redirected to it in response to an attack on a specific target.

Arbor TMS comes in a variety of mitigation platforms and capacities including: 2U appliances (500 Mbps–400 Gbps of mitigation), 6U chassis (10–100 Gbps of mitigation), Cisco ASR 9000 Router embedded (10–60 Gbps of mitigation) and virtual supporting KVM & VMware hypervisor (1– 40 Gbps).



Comprehensive Threat Detection

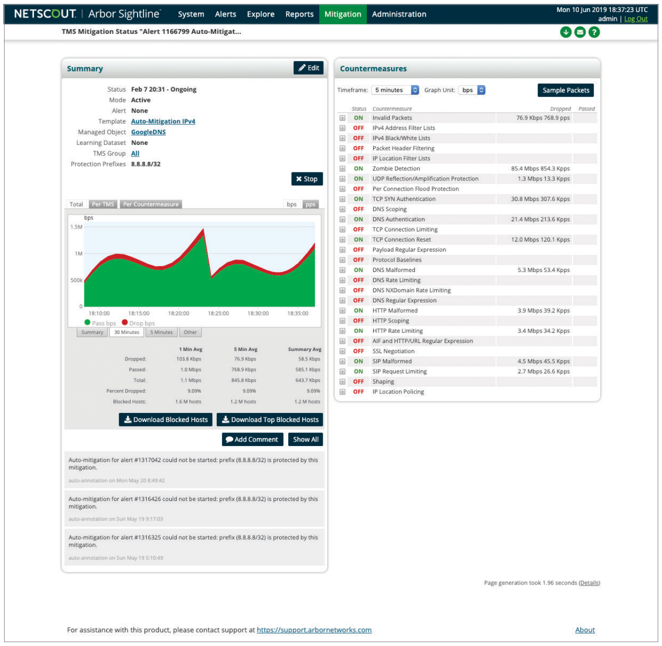
Data centers and public networks present multiple targets for DDoS attacks. These targets include infrastructure devices (e.g., routers, switches and load balancers), Domain Name Systems (DNS), bandwidth capacity and key applications such as web, eCommerce, voice and video. Even security devices such as Firewalls and Intrusion Prevention Systems are targets of attack. The Arbor solution provides the most comprehensive and adaptive suite of threat detection capabilities in the industry, designed to protect diverse resources from complex, blended attacks. These capabilities include statistical anomaly detection, protocol anomaly detection, fingerprint matching and profiled anomaly detection. Our solution continually learns and adapts in real-time, alerting operators to attacks, as well as to unusual changes in demand and service levels.

Surgical Mitigation in Seconds

Key to effective mitigation is the ability to identify and block attack traffic while allowing non-attack traffic to flow through to its intended destination. Large-scale DDoS attacks affect not only the intended victim, but also other unfortunate customers who may be using the same shared network service. To reduce this collateral damage, Service Providers and Hosting providers often shut down all traffic destined for the victim's site, thus completing the DDoS attack. Whether it's a high-volume flood attack designed to exhaust bandwidth capacity or a targeted attack looking to bring down a website, in some cases, Arbor TMS can isolate and remove the attack traffic, without affecting other users, in as fast as a few seconds. Methods include identifying and black-listing malicious hosts, IP location-based mitigation, protocol anomaly-based filtering, malformed packet removal and rate limiting (to gracefully manage non-malicious demand spikes). Mitigations can be automated or operator-initiated and countermeasures can be combined to address blended attacks.

Real-Time Mitigation Dashboard

Arbor TMS real-time mitigation dashboard is a single screen that shows operators exactly what is generating a DDoS alert and what effect the countermeasures are having on the attack. It provides the ability to modify countermeasures and delivers full packet capture and decode to get a detailed view of both normal and attack packet streams. This information is stored for future reference and management reporting — giving operators and managers full visibility and reporting into attacks on their business operations.



Mon 10 Jun 2019 18:37:23 UTC

TMS Mitigation Status "Alert 1166799 Auto-Mitigat...

Summary

Status	Feb 7 20:31 - Ongoing
Mode	Active
Alert	None
Template	Auto-Mitigation IPv4
Managed Object	GoogleDNS
Learning Dataset	None
TMS Group	All
Protection Prefixes	8.8.8.8/32

	1 Min Avg	5 Min Avg	Summary Avg
Dropped:	103.8 Kbps	76.9 Kbps	58.5 Kbps
Passed:	1.0 Mbps	768.9 Kbps	585.1 Kbps
Total:	1.1 Mbps	845.8 Kbps	643.7 Kbps
Percent Dropped:	9.09%	9.09%	9.09%
Blocked Hosts:	1.6 M hosts	1.2 M hosts	1.2 M hosts

Auto-mitigation for alert #1317042 could not be started: prefix (8.8.8.8/32) is protected by this mitigation.

auto-annotation on Mon May 20 8:49:42

Auto-mitigation for alert #1316426 could not be started: prefix (8.8.8.8/32) is protected by this mitigation.

auto-annotation on Sun May 19 9:17:03

Auto-mitigation for alert #1316325 could not be started: prefix (8.8.8.8/32) is protected by this mitigation.

auto-annotation on Sun May 19 5:10:49

Countermeasures

Timeframe: 5 minutes Graph Unit: bps

Status	Countermeasure	Dropped	Passed
ON	Invalid Packets	76.9 Kbps 768.9 pps	
OFF	IPv4 Address Filter Lists		
OFF	IPv4 Black/White Lists		
OFF	Packet Header Filtering		
OFF	IP Location Filter Lists		
ON	Zombie Detection	85.4 Mbps 854.3 Kpps	
ON	UDP Reflection/Amplification Protection	1.3 Mbps 13.3 Kpps	
OFF	Per Connection Flood Protection		
ON	TCP SYN Authentication	30.8 Mbps 307.6 Kpps	
OFF	DNS Scoping		
ON	DNS Authentication	21.4 Mbps 213.6 Kpps	
OFF	TCP Connection Limiting		
ON	TCP Connection Reset	12.0 Mbps 120.1 Kpps	
OFF	Payload Regular Expression		
OFF	Protocol Baselines		
ON	DNS Malformed	5.3 Mbps 53.4 Kpps	
OFF	DNS Rate Limiting		
OFF	DNS NXDomain Rate Limiting		
OFF	DNS Regular Expression		
ON	HTTP Malformed	3.9 Mbps 39.2 Kpps	
OFF	HTTP Scoping		
ON	HTTP Rate Limiting	3.4 Mbps 34.2 Kpps	
OFF	AIF and HTTP/URL Regular Expression		
OFF	SSL Negotiation		
ON	SIP Malformed	4.5 Mbps 45.5 Kpps	
ON	SIP Request Limiting	2.7 Mbps 26.6 Kpps	
OFF	Shaping		
OFF	IP Location Policing		

Page generation took 1.96 seconds (Details)

For assistance with this product, please contact support at https://support.arbornetworks.com

Real-time alerting and mitigation dashboard.

MULTIPLE METHODS OF THREAT DETECTION AND MITIGATION

Block known malicious hosts by using white and black lists

The white list contains authorized hosts, while the black list contains zombies or compromised hosts whose traffic will be blocked.

Block application-layer exploits by using complex filters

Arbor TMS provides payload visibility and filtering to better ensure cloaked attacks cannot bring down critical services.

Defend against web-based threats by detecting and mitigating HTTP-specific attacks

These mechanisms also help with managing flash-crowd scenarios.

Protect critical DNS services

from cache poisoning, resource exhaustion and amplification attacks. Add greater visibility into DNS services.

Protect VoIP services

from automated scripts or botnets that exploit packet-per-second and malformed request floods by employing VoIP/SIP-specific attack detection and mitigation capabilities.

Stop large reflection/amplification attacks

Such as NTP, DNS, Memcached, SNMP, SSDP, SQL RS or Chargen by leveraging up to 400 Gbps of attack mitigation in a single Arbor TMS chassis.

Scalable DDoS Attack Detection and Mitigation

Arbor SP scales on physical and virtual instances to provide comprehensive DDoS detection across an entire Service Provider network, from the customer edge to the peering edge to the data center edge (or cloud edge) to the mobile edge, including the backbone network in-between. With this unparalleled visibility, Arbor SP's workflows enable quick effective mitigation of any DDoS attack via Arbor TMS or Cisco ASR 9000 vDDoS protection. Countermeasure based mitigations scale up to 400 Gbps per TMS HD1000 and up to 8 Tbps in a deployment. Blacklisting unlocks an additional layer of protection ahead of any countermeasure mitigations. The Cisco ASR 9000 vDDoS protection solution uses OpenFlow to blacklist at massive scale of up to tens of Tbps of protection at any edge of your network and thereby safeguarding your core links from attack.

Comprehensive Management and Reporting

Arbor TMS simplifies and streamlines operations by providing the ability to view and manage up to eight terabits of mitigation capacity from a single point of control. This provides the ability to thwart multiple, large-scale attacks and produce comprehensive reports that summarize the mitigation process for customers and/or management.

A Platform for Managed DDoS Services

The Arbor solution enables Service Providers and Hosting/Cloud providers to deliver DDoS protection services to their customers. Customized portal access, APIs and delegated management give Managed Service Providers (MSPs) the flexibility and control to tailor services to fit their customers' needs. Arbor is the undisputed leader for managed DDoS protection. It is the solution of choice for the vast majority of leading DDoS managed services.

Arbor TMS DDoS Defense Specifications

Simultaneous Sessions	Not session limited	
Deployment Modes	Inline Active, Inline Monitoring, SPAN port, Diversion/Reinjection	
Block Actions	Source blocking/source suspend; per packet blocking; combination of source, header and rate based blocking; Automated BGP Flowspec Source/Destination Blocking	
Attack Protections	Reflection Amplification Flood Attacks (TCP, UDP, ICMP, DNS, mDNS, Memcached, SSDP, NTP, NetBIOS, RIPv1, rpcbind, SNMP, SQL RS, Chargen, L2TP, Microsoft SQL Resolution Service); Fragmentation Attacks (Teardrop, Targa3, Jolt2, Nestea); TCP Stack Attacks (SYN, FIN, RST, ACK, SYN-ACK, URG-PSH, other combinations of TCP Flags, slow TCP attacks); Application Attacks (HTTP GET/POST Floods, slow HTTP Attacks, SIP Invite Floods, DNS Attacks, HTTPS Protocol Attacks); SSL/TLS Attacks (Malformed SSL Floods, SSL Renegotiation, SSL Session Floods); DNS Cache Poisoning; Vulnerability Attacks; Resource Exhaustion Attacks (Slowloris, Pyloris, LOIC, etc.); Flash Crowd Protection; Attacks on Gaming Protocols	
DDoS Countermeasure	**Volumetric-Only Countermeasures**	**Full Set of Countermeasures**
	Invalid Packets, IP Address Filter Lists, Black/White Filter Lists, Packet Header Filtering, IP Location Filter Lists, Zombie Detection, UDP Reflection/Amplification Protection, Per Connection Flood Protection, Spoofed TCP SYN Flood, TCP SYN Authentication, TCP Connection Limiting, TCP Connection Reset, Payload Regular Expression Filter, Shaping, IP Location Policing, Inline Filter, Blacklist Fingerprints, Protocol Baselines	HTTP Authentication, HTTP Malformed, HTTP Scoping, HTTP Rate Limiting, HTTP/URL Regular Expression, DNS Authentication, DNS Malformed, DNS Scoping, DNS Rate Limiting, DNS Regular Expression, SIP Malformed, SIP Request Limiting, SSL Negotiation, ATLAS Intelligence Feed (AIF)

ATLAS INTELLIGENCE FEED

Leveraging a global network of traffic monitoring and sensors, Arbor researchers have developed ATLAS® Intelligence Feed, a library of targeted defenses providing automatic protection from the vast majority of botnet-based attacks. ATLAS Intelligence Feed automatically updates Arbor TMS with new protections as Arbor researchers find and neutralize emerging threats.

Arbor TMS 2600, 2800, 5000, and HD1000 Specifications

	Arbor TMS 2600	Arbor TMS 2800	Arbor TMS 5000	Arbor TMS HD1000
Throughput and Mitigation *2600 and 2800 series are software license*	Licenses for 1 Gbps, 2 Gbps, 5 Gbps, 10 Gbps (add-on to 20 Gbps) all up to 15 Mpps	Licenses for 10 Gbps, 20 Gbps, 30 Gbps, 40 Gbps, all up to 30 Mpps	**1 x APMe:** Up to 25 Gbps, 10 Mpps **2 x APMe:** Up to 50 Gbps, 20 Mpps **3 x APMe:** Up to 75 Gbps, 30 Mpps **4 x APMe:** Up to 100 Gbps, 40 Mpps	Up to eight Packet Processing Modules (PPMs); Any combination of 20 Gbps (14Mpps) or 50 Gbps (25 Mpps) of mitigation throughput, Maximum 400 Gbps, 198 Mpps
Power Requirements	Redundant Power Supplies **AC:** 100-240 VAC, 50/60 Hz, 12/6 A max.; **DC:** -40 to -72 Vdc, 28/14 A max.	Redundant Power Supplies **AC:** 100-240 VAC, 50/60 Hz, 12/6 A max.; **DC:** -40 to -72 Vdc, 28/14 A max.	Redundant Quad Power Supplies **AC:** 100-120 VAC/ 200-240 VAC, 50 to 60Hz, 15A; **DC:** -48/-60 Vdc, 90A max	**AC:** Two 1500-watt redundant power supplies; 100-240V AC, 15-10 A, 50-60 Hz (x2); **DC:** Two 1500-watt redundant power supplies; -48 to -60 V dc, 44 A (x2)
Power Requirements and Heat	325 Watts (max.), 280 Watts (nom.): @ 280 Watts, 955 BTU/hr	325 Watts (max.), 280 Watts (nom.): @ 280 Watts, 955 BTU/hr	**1xAPMe:** 1090 Watts (max.), @ 610 Watts (nom.) 2081 BTU/hr **2x APMe:** 1125 Watts max., @ 800 Watts nom. 2730 BTU/hr **3 x APMe:** 1440 Watts max., @ 980 Watts nom. 3344 BTU/hr 4 **x APMe:** 1595 Watts max., @ 1160 Watts nom. 3958 BTU/hr	(1) MM, (5) fans, (2) QSFP+, (4) QSFP28; (x1) PPM: @ 327 Watts, 1116 BTU/ hr; (x4) PPM: @ 569 Watts, 1940 BTU/ hr ; (x8) PPM: @ 932 Watts, 3180 BTU/ hr
Dimensions	**Chassis:** 2U rack height **Weight:** 36.95 lbs (17.76 kg) **Height:** 3.45 in (8.76 cm) **Width:** 17.14 in (43.53 cm) **Depth:** 20 in (50.8 cm)	**Chassis:** 2U rack height **Weight:** 39 lbs (17.7 kg) **Height:** 3.45 in (8.76 cm) **Width:** 17.14 in (43.53 cm) **Depth:** 20 in (50.8 cm)	**Chassis:** 6U rack height **Weight:** With AC: 77.15 lb (34.99 kg); With DC: 58.52 lb (26.54 kg); Add 6 lb (2.72 kg) per APM-E blade **Height:** 10.463 in (26.58 cm) **Width:** 19.00 in (48.26 cm) **Depth:** 18.19 in (46.20 cm) with handles	**Chassis:** 2U rack height **Weight:** 45.2 lbs (20.5 kg) with 1 PPM, add 1.6 lb (.73 kg) per PPM (up to eight) **Height:** 3.5 in (8.89 cm) **Width:** 17.6 in (44.70 cm) **Depth:** 21 in (53.34 cm)

Network Interfaces	4x10G (SFP+) + 8x1G (SFP) ports	8 x 10 GigE (SFP+ for SR or LR or mixed fiber)	32 x 10 GigE (QSFP+ with breakout cables, SR4 or 4LR);
			8 x 40 GigE (QSFP+ SR4 or LR4);
			4 x 100 GigE (LR4)
				4x100G + 8x10G = One to four 100 GbE QSFP28 (LR) optical transceivers + One or two 4 x 10 GbE QSFP+ (SR or LR Lite) optical transceivers with one 4 x 10 GbE breakout cable on each transceiver
				16x10G = One to eight 10 GbE SFP+ (SR or LR) optical transceivers + One or two 4 x 10 GbE QSFP+ (SR or LR Lite) optical transceivers with one 4 x 10 GbE breakout cable on each transceiver

Storage	2x150GB SSD drives, RAID 1	2x240GB SSD drives, RAID 1	2x128GB SSD drives, RAID 1	2x480GB SSD drives, RAID 1
Environmental	**Operating temperature:** 41° to 104°F (5° to 40°C) **Relative humidity (operating):** 5 to 85% non-condensing	**Operating temperature:** 41° to 104°F (5° to 40°C) **Relative humidity (operating):** 5 to 85%, (non-operating) 95% at 73° to 104°F (23° to 40°C)	**Operating temperature:** 23° to 104°F (-5° to 40°C) **Relative humidity (operating):** 5% to 85% non-condensing	**Operating temperature:** 39.2° to 104°F (-4° to 40°C)

	Arbor TMS 2600	Arbor TMS 2800	Arbor TMS 5000	Arbor TMS HD1000
Regulatory	UL60950-1/CSA 60950-1 (USA/Canada); EN60950-1 (Europe); IE60950 (International), CB Certificate & Report including all international deviations; GS Certificate (Germany); EAC-R Approval (Russia); CE – Low Voltage Directive 73/23/EEE (Europe); BSMI CNS 13436 (Taiwan); KCC (South Korea); RoHS Directive 2002/95/EC (Europe)	UL 60950-1 2nd edition/ CSA C22.2 No. 60950-1-07 2nd Edition, Low Voltage Directive 2006/95/EC, Safety Directive 2001/95/EC, CB Certificate and Report to IEC60950-1, 2nd edition and all international deviations, FCC 47CFR Parts 15, Verified Class A limit, ICES-003 Class A Limit, EMC Directive, 2004/108/EC, EN55022, EN55024, EN61000-4-2, EN61000-4-3, EN61000-4-4, EN61000-4-5, EN61000-4-6, EN61000-4-8, EN61000-4-11,EN61000-3-2, EN61000-3-3, VCCI Class A ITE (CISPR 22, Class A Limit), BSMI Approval, CNS 13438, Class A and CNS13436 Safety, KCC Approval, Gost Approval, CISPR 22 Class A Limit, CISPR 24 Immunity, RoHS (recast) Directive 2011/65/EU	RoHS 6/6, IEC/EN/UL 60950-1, FCC Part 15 Subpart B Class A, ETSI EN 300 386, UL Mark, CE Mark	RoHS 6/6, IEC/EN/UL/ CSA 60950-1, FCC Part 15 Subpart B Class A, EN 55022, EN55024, ETSI EN 300 386, cCSAus Mark, CE Mark, KN22, KN24, RCM Mark, KCC Mark, EAC Mark, BIS, CCC Mark (pending).
Hardware Bypass	External			

Virtual TMS (vTMS)

Supported Hypervisor	VMware or KVM running on any modern Linux distribution, x86_64
Virtual Machine Specifications	**Cores:** 3-32, RAM: 9.5-56GB, **Mitigation Interfaces:** 1-8, Management Interfaces: 1-2
Configuration Mitigation Throughput	**3 Core without hardware passthrough:** 3 vCPU, 9.5G RAM, 100GB of disk space, 2 virtio management interfaces, 2 virtio mitigation interfaces = 1 Gbps **3 Core with hardware passthrough:** 3 vCPU, 9.5G RAM, 100GB of disk space, 2 virtio management interfaces, 8 Intel 82599 PCI Passthrough mitigation interfaces = 6 Gbps **16 Core with hardware passthrough:** 16 vCPU, 29G RAM, 100GB of disk space, 2 virtio management interfaces, 8 Intel 82599 PCI Passthrough mitigation interfaces = 40 Gbps
Supported NFV Management and Orchestration	Openstack (Heat, Tracker), Ansible, Cisco NSO/ESC, Nokia CloudBand, AWS CloudFormation

NETSCOUT

Corporate Headquarters
NETSCOUT Systems, Inc.
Westford, MA 01886-4105
Phone: +1 978-614-4000
www.netscout.com

Sales Information
Toll Free US: 800-309-4804
(International numbers below)

Product Support
Toll Free US: 888-357-7667
(International numbers below)

NETSCOUT offers sales, support, and services in over 32 countries. Global addresses, and international numbers are listed on the NETSCOUT website at: www.netscout.com/company/contact-us