A10 DDOS PROTECTION CLOUD

A10 Networks provides full spectrum DDoS defenses. This includes multi-vector protection from attacks of any type to ensure the availability of enterprise business services. The combination of a surgically precise, on-premise appliance along with orchestrated cloud scrubbing is delivered in cost-efficient form-factors and subscription models.

FULL SPECTRUM ENTERPRISE DDOS PROTECTION

With the increase in sophistication, intensity and frequency of DDoS attacks, enterprises are realizing that cloud DDoS scrubbing is a good option, but not a panacea by itself. A hybrid approach delivers the best protection. Cloud scrubbing is most effective when attack volume grows beyond the capacity of an enterprise's internet pipe. Yet enterprises need to complement their cloud solutions with the surgical precision and context-aware controls offered by A10's on-premise DDoS defenses. These defenses protect users and applications from more frequent, smaller, and sophisticated attacks with always-on and instant protection. These attacks can overwhelm resources on applications, services and security equipment, and distract IT staff from real attacks that are happening. These attacks result in application downtime, wasted IT resources and security overspend, and should not be permitted to enter and disrupt the enterprise network.

DDoS Protection Cloud protects your organization when volumetric attacks grow past your internet bandwidth capacity. It works in concert with A10 Thunder TPS® and is delivered as a service orchestrated by A10 DDoS Security Incident Response Team (DSIRT).

DDoS Protection Cloud is a cost-effective DDoS defense solution. Other DDoS scrubbing services charge based on DDoS attack traffic volumes. With DDoS Protection Cloud, you pay only for legitimate traffic, the number of routers protected and the number of times cloud-scale scrubbing is needed. There are no hidden fees based on the number of network segments or geographic locations. And because A10 Thunder TPS (Threat Protection System) deflects all attacks that fall under your on-premise internet bandwidth, A10's two-pronged hybrid defense is the most effective and economical full spectrum DDoS defense solution.

PRODUCTS AND SERVICES

DSIRT

DDOS PROTECTION CLOUD

ON-PREMISE APPLIANCES

THUNDER TPS
Physical Appliance

vTHUNDER TPS
Virtual Appliance

aGALAXY
Management

TALK
WITH A10

WEB
a10networks.com/tps

CONTACT US
a10networks.com/contact

BENEFITS

MAINTAIN
SERVICE AVAILABILITY

Downtime results in immediate productivity and revenue loss for any business. A10's hybrid DDoS protection solution ensures service availability by spotting anomalies automatically across the traffic spectrum and mitigating multi-vector DDoS attacks of any type.

DEFEAT
GROWING ATTACKS

Our hybrid DDoS solution protects the most demanding network environments. Thunder TPS offloads common attack vectors to specialized hardware, allowing its powerful, multicore CPUs to distinguish legitimate users from attacking botnets and complex application-layer attacks that require resource-intensive deep packet inspection (DPI). When attacks grow past an organization's internet bandwidth capacity, DSIRT orchestrates traffic redirection to DDoS Protection Cloud for traffic scrubbing.
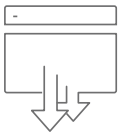
DEPLOY
WARTIME SUPPORT

No organization has unlimited trained personnel or resources during real-time DDoS attacks. Thunder TPS supports five levels of programmatic mitigation escalation and de-escalation per protected zone. This eliminates the need for frontline personnel to make time-consuming manual changes to escalating mitigation strategies and improves response times during attacks. Administrators have the option to manually intervene as well as to coordinate with A10's DSIRT, a team of trained security personnel, to redirect network traffic to DDoS Protection Cloud for volumetric attack scrubbing.

REDUCE
SECURITY OPEX

A10 DDoS Protection Cloud service is built to protect your legitimate traffic, not for the amount of traffic that attacks apply against you. You are only charged for the protected traffic and the number of times cloud-scale scrubbing is required. There are no hidden charges for the number of network segments or geographic locations to be protected.

REFERENCE ARCHITECTURES
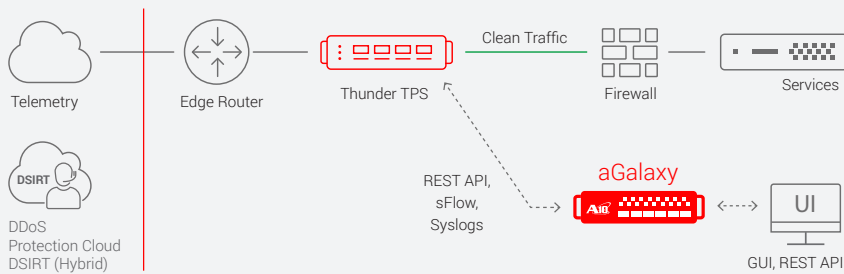
PROACTIVE MODE

Proactive on-premise mode provides continuous, comprehensive detection and faster mitigation. This mode is most useful for environments where user experience and application performance is critical. TPS supports L2 or L3 inline deployments. L3 deployment eliminates the need for network interruption during installation or required maintenance windows. A10 DSIRT orchestrates traffic redirection on an on-demand basis.
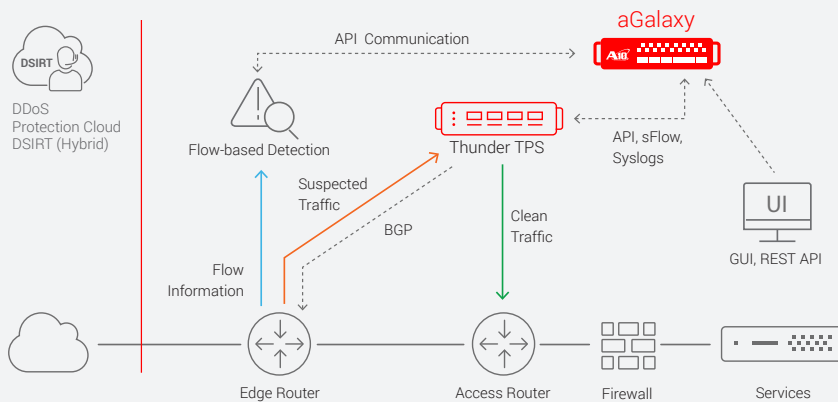
REACTIVE MODE

Larger networks benefit from reactive on-premise mitigation, triggered by Thunder TPS Detector from edge router flow records. TPS fits in any network configuration with integrated BGP and other routing protocols. DSIRT orchestrates traffic redirection on an on-demand basis.

FEATURES

COMPLETE HYBRID
DDOS SOLUTION

A single-vendor solution for DDoS protection through surgical precision on-premise, cloud scrubbing, redirection orchestration, support and professional services.

COST EFFECTIVE
HYBRID DDOS SOLUTION

You're charged only for the protected traffic not the amount of attack traffic. No additional cost for number of IP blocks protected.

FULL SPECTRUM
PROTECTION

Application, network and sophisticated attack protection on-premise with volumetric DDoS attack cloud scrubbing.

MAINTAIN CONTROL
OVER APPLICATION PROTECTION

Flexible controls over on-premise defenses tuned to your legitimate users application access.

SCALE
FOR VOLUMETIC ATTACKS

The service is backed by purpose-built, globally distributed scrubbing centers scaled to handle the largest known DDoS volumetric attacks, all orchestrated by A10 DSIRT.

EASY NETWORK
INTEGRATION

Support for BGP and DNS cloud redirection.
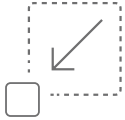
24-7
PROTECTION SUPPORT

Spin up 24-7 DDoS attack support from the A10 DSIRT, included with A10 support.

ORCHESTRATED
CLOUD REDIRECTION

Respond faster and minimize outages with (DSIRT) orchestrated cloud redirection.

Features (Cont.)

SMALL, EFFECTIVE ON-PREMISES FOOTPRINT

Thunder TPS's surgical detection and mitigation is available as a virtual appliance or as hardware appliances ranging from 2 Gbps to 152 Gbps mitigation bandwidth in just 1 RU form factor.

powered by **VERISIGN**

A10 leverages the market proven Verisign DDoS protection platform to deliver a full spectrum DDoS protection solution.

SERVICE DELIVERY OPTIONS

	95% AGGREGATE CLEAN TRAFFIC VOLUME	*LIMITED CLOUD REDIRECTION OPTION* (per year)	*UNLIMITED CLOUD REDIRECTION OPTION AVAILABLE*
Clean Traffic Volume Categories (Mbps)	20	4	Yes
	50	8	
	100	8	
	500	12	
	1,000	12	
	2,000	12	
	4,000	12	
	6,000	12	
	8,000	12	
	Contact A10 for greater than 8,000 Mbps		
Number of Routers Protected	Pricing based on number of routers protected (for BGP redirection mode)		
Mitigation Interval	Each mitigation includes up to 48 hours of usage. Usage beyond 48 hours, will be automatically counted as more than one mitigation.		

Traffic Redirection Modes

- BGP with redundant GRE tunnel return path
  - Unlimited protection for all IP blocks at no additional charge
- DNS
  - 5 protected VIPs for 500 Mbps clean traffic or less categories
  - 10 protected VIPs for 1000 Mbps clean traffic or more categories
  - Additional protected VIPs available

Thunder TPS On-Premises

- In-line packet-based DDoS detection
- Out-of-band flow-based DDoS detection
- Peacetime behavioral learning
- Manual and learned thresholds
- A10 DDoS Threat Intelligence, included with support
- Application attack protection
  - Application-aware filter
  - Regular expression filter (TCP/ UDP/HTTP)
  - HTTP request rate limit (per URI)
  - DNS request rate limit (per type)
  - DNS query check
  - DNS domain-list
  - HTTP protocol compliance
  - Application (DNS/HTTP) flood protection
  - Amplification attack protection

- Resource attack protection
  - SYN Flood
  - Fragmentation attack
  - Slowloris
  - Slow GET/POST
  - Long form submission
  - SSL renegotiation
- Protocol attack protection
  - Invalid packets
  - Anomalous TCP flag combinations (no flag, SYN/FIN, SYN frag, LAND attack)
  - IP options
  - Packet size validation (ping of death)
  - POODLE attack
  - TCP/UDP/ICMP flood protection
  - Per-connection traffic control

LEARN MORE
ABOUT A10 NETWORKS

CONTACT US
a10networks.com/contact