AVX SERIES SOLUTION BRIEF

DDoS

DDoS functions for basic on-premises L2-L3 packet/connection scrubbing for volume traffic and on-premises, on-demand scrubbing via routing protocols.

Array DDoS Overview

DDoS attacks can be an IT department's worst nightmare. By combining high-volume traffic clogging with application-targeted techniques, these stealthy attacks can disrupt service for legitimate users, or take down applications or even entire networks.

In the past, organizations had only two options for handling DDoS attacks: black-holing or scrubbing with 3rd-party service providers. Black-holing is a common defense technique to stop DDoS attacks by blocking incoming traffic and redirecting it into a "black hole" or null route. A scrubbing technique uses a centralized data cleansing station where the incoming traffic is analyzed and malicious traffic is removed before it is sent to the destination.

Typically, DDoS mitigation services are either on-demand or always on. On-demand solutions can be started either manually or automatically by the IT manager or in some instances, the vendor, when a DDoS attack is detected. Network traffic is then rerouted via DNS redirection or GBP route changes through the vendor's DDoS protection services.

Always-on DDoS protection does not require DNS or routing changes, and is often deployed when there has been a history of frequent DDoS attacks. According to vendors of this type of product, there is only a minor impact on application latency, and may be especially useful for content delivery applications and services.

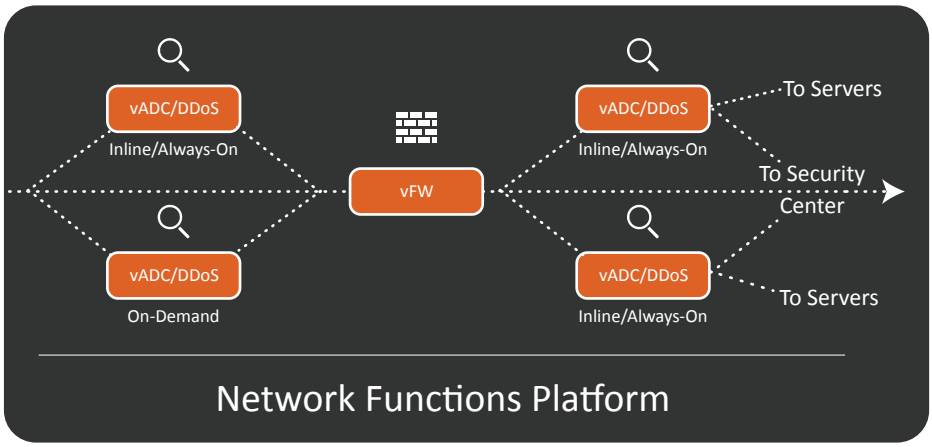
By contrast, hybrid solutions offer the best attributes of both on-demand and always-on solutions. This type of solution allows IT managers to leverage on-premise devices such as network and web application firewalls for DDoS filtering as the first layer of defense. If the attack is prolonged or intensive, traffic can be redirected to a vendor's off-site facility for additional remediation.

Array's DDoS capabilities provide a hybrid solution that offers the best of both worlds. DDoS technology as well as other security capabilities are available as hardware appliances that support traffic up to 100Gbps or as virtual appliances on industry-standard hypervisors and Array's AVX Series Network Functions Platform.

Array Networks DDoS is typically deployed on-premises, in-line and always on in front of web or application servers. Where performance could potentially be an issue, such as more granular and more focused deep packet processing, SSL termination, L7 protections and rate limiting which consume much higher CPU, physical appliances may be most suitable for distinguishing legitimate user requests from attackers. Array Networks DDoS can be deployed in conjunction with other Array platforms or third party platforms for application availability and scaling.

Array Networks DDoS functions can be deployed similar to other general DDoS products, doing basic on-premises L2-L3 packet/connection scrubbing for volume traffic. In addition, Array Networks DDoS can utilize routing protocols to support on-premises, on-demand scrubbing.

The following diagram illustrates possible Array Networks DDoS deployments:



WebWall®, Array's suite of web application security capabilities, can protect against distributed denial of service (DoS/DDoS) and malformed URL attacks and allow a wide range of Layer 2 through Layer 7 protective policies to be stacked atop one another for increased security.

The Array Networks solution is security-hardened to protect applications and servers from L4 and L7 DDoS attacks and support content filtering to guard against protocol and application DDoS attacks as well as Syn-flood, tear drop, ping-of-death, Nimda, Smurf and other malicious attacks. The Array solution also features extensive access control lists, network address translation and stateful packet flow inspection – all executed at the kernel level – to guard against attacks and unauthorized access without impacting performance or scalability.

In addition, WebWall provides deep application data inspection – beyond IP and TCP headers – to deal with attacks such as SQL injection and cross-site scripting. Deployable in front of multiple web or application servers, Array's web application firewall detects and responds to signatures for known application vulnerabilities and is programmable to deal with future threats.

DDoS Defense Benefits

- Broad, multi-layer DDoS protection at the application, session and network layers
- Machine learning of traffic patterns allows automatic detection of anomalous traffic and auto-configuration of thresholds
- Protects against common DDoS attack types as well as zero-day attacks
- Flexible deployment options – inline/always-on or on-demand,
- Extensive access control lists, network address translation and stateful packet flow inspection, all executed at the kernel level, to guard against attacks and unauthorized access without impacting performance or scalability
- Also provides load balancing across multiple servers to assure high availability and user experience
- Multiple deployment options: on Array's Network Functions Platform, on Array APV Series dedicated load balancers or vAPV virtual load balancers

Array Networks DDoS Protection

Array Networks DDoS protection includes multi-layer protection across network, session and application layers:

	Types of Attacks	Array Networks DDoS Technology Capabilities
Application	Volumetric overload attack. OWASP Top 10 (SQL injection, XSS, CSRF, etc.), Slowloris, Slow/long Post, HashDos, Get floods	Web acceleration/high capacity, Individual application control, scale up/down application capacity, flash event handling. Full proxy for HTTP/TCP/FTP/SIP/DNS, etc., policy reinforcement, threshold auto configuration, abnormality detection, suspect client filtration, BOT detection, URL filtering, request rate limiting, DDoS Log.
Session	TCP flooding, DNS UDP floods, DNS query floods, DNS NXDOMAIN floods, SSL floods, SSL renegotiation	TCP Termination, buffering, sync-cookie. High-capacity connection table. SSL termination, client access statistics gathering, state timers, connection rate limit, logs. white list, dynamic black list.
Network	SYN floods, connection floods, UDP floods, PUSH and ACK floods, teardrop, ICMP floods, ping floods, smurf, and IP option attacks.	Secured/Hardened ArrayOS, SpeedCore high-speed packet processing, WebWall - stateful firewall, IP filtering, RFC check, real-time IP statistics.

Conclusion

Array Networks DDoS protection provides a high-performance on-premises solution that can effectively deal with DDoS attacks and flash events, keeping applications available to legitimate users while mitigating possible attacks.

For more information about how Array Networks can help you protect against DDoS attacks, visit us at arraynetworks.com or send us an email at sales-info@arraynetworks.com.

1371 McCarthy Blvd., Milpitas, CA 95035 | Phone: (408) 240-8700 | Toll Free: 1-866-MY-ARRAY | www.arraynetworks.com