Product Specifications: DefenseFlow Network and Services DDoS Protection

FEATURE/CAPABILITY	DefenseFlow
ATTACK DETECTION	
Detection Methods	• Adaptive behavioral detection engine o Adaptive engine creating normal traffic baselines per protected object or single host for rate, rate-invariant and avg. packet size traffic parameters o Adaptive expert system detects attacks based on deviations from normal baselines per protected object or single host and traffic type • DefensePro as a Detector (DPaaD) in always-on/SmarTap deployment • Manual detection mode based on traffic rate-based threshold • Indications from external security devices
Type of Attacks Detected	• Behavioral detection engine o TCP network flood attacks o UDP network flood attacks o ICMP network flood attacks o Other: IP floods • DPaaD o Volumetric and non-volumetric attacks, SYN-flood attacks, low-and-slow attacks, HTTP floods, SSL-based attacks, and more
SECURITY PROTECTION SETTINGS	
Protected Object - Supported Network Classification Per Policy	• IP address or IP addresses set • IP subnet mask, CIDR • Virtual network ID: VLAN
Number of Protected Objects Supported Per Defenseflow	10,000
Number of Protected Hosts Supported Per Defenseflow Behavioral Detection	5000 divided in up to 5 protected objects
MANAGEMENT & MONITORING	
Configuration Management Interface	REST API, CLI, and Web UI
Security Logs Interface	Web UI
Security Logs Sources	Collected from DefenseFlow and DefensePro mitigation devices to provide unified event log view
Real-Time Traffic Monitoring Statistic Interface	Web UI
OUT-OF-PATH DEPLOYMENT	
Number of Supported Radware's DefensePro Mitigation Devices	40
Protected Object Baseline Synchronization with Radware's DefensePro Mitigation Device	Automatic
Policy Synchronization with Radware's DefensePro Device	Automatic
Policy and Baselines Delegation from DefensePro to DefensePro	Automatic
"SHORT" TRAFFIC REDIRECTION	One hop traffic redirection
Traffic Redirection to Local Mitigation Device	Supported for both SDN and BGP redirection
Traffic Redirection to Local Tap Device	Support diverting from detection only device to mitigation
Traffic Redirection Granularity	Suspected traffic type per attacked destination or entire protected object
Short Traffic Redirection Modes	Ingress only
"LONG" TRAFFIC REDIRECTION	Traffic redirection to a remote mitigation device (scrubbing center) connected anywhere in the network
Traffic Redirection to Remote Mitigation Device	Supported for both SDN and BGP redirection
Traffic Redirection Granularity	Suspected traffic type per attacked destination or entire protected object
ATTACK MITIGATION	
DP Mitigation Device Version	DefensePro version 7.x and 8.x
Clustering of Mitigation Devices	Yes
Traffic Blocking	BGP BH, Flowspec
ENVIRONMENT COMPATIBILITY	
xFlow Statistics Collectors Support	Radware's Flow Collector version 8.02.05
External Detectors	Pluggable API to 3rd party detectors, detection REST API

Software Specifications

FEATURE/CAPABILITY	DefenseFlow
SOFTWARE SPECIFICATIONS	
Supported Environments	KVM and VMware ESXi 5.x
MINIMUM REQUIREMENTS FOR VA OVER KVM	
Memory	16 GB
Hard Drive	50 GB
Processors	4 cores