DefenseFlow: The SDN Application that Programs Networks for DoS Security

Radware's DefenseFlow™ is an SDN application that enables network operators to program the network to provide DDoS protection as a native network service. DefenseFlow features an adaptive behavioral-based DoS attack detection engine and a traffic diversion mechanism that utilizes the programmable characteristics of the software defined network elements for attack cleansing. Designed as part of the Radware SDN application framework, DefenseFlow operates in any SDN enabled network infrastructure.

Network Applications in Software Defined Networking (SDN)

Software Defined Networking (SDN) is a network architecture where network control is decoupled from forwarding and is directly programmable. This migration of control, formerly coupled with network devices, is a software-based centralized control entity that enables the network infrastructure to be abstracted for the purpose of applications and network services which can treat the network as a logical entity. Figure 1 shows DefenseFlow as an SDN application that enables the network to be programmed with a native DDoS protection service through the SDN controller northbound interface.

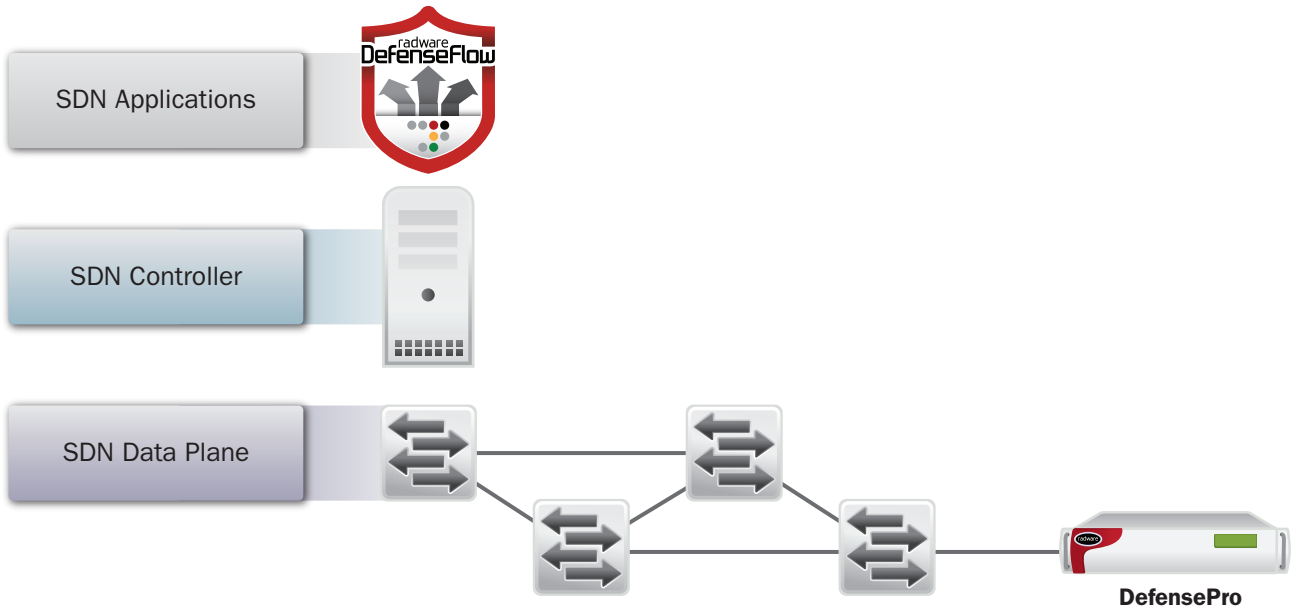


Figure 1 – DefenseFlow is a network DDoS attack detection and traffic diversion application deployed in the SDN application layer

Following Radware's SDN strategy, DefenseFlow transforms DDoS protection from device-based into network-wide services by utilizing SDN control plane to collect and control the data plane. DefenseFlow introduces unique behavioral-based technology to detect network attacks in real time - a level of intelligence that increases the value that can be extracted from the networks at a very low cost.

Proactive DDoS Protection as an SDN Application

DefenseFlow is a software product that leverages SDN technologies to provide DoS & DDoS protection as a native network service. It uses the programmability of SDN technologies to collect statistics, analyze the information and control the infrastructure layer to proactively defend against DoS & DDoS network flood attacks and to automate the provisioning of an attack mitigation service.

DefenseFlow offers widest network DDoS attacks coverage:

- SYN floods
- TCP floods
- UDP floods
- ICMP floods
- IGMP floods
- Fragmented packet floods
- Out-of-state floods
- Network and port scanning

Collect: Network-wide Statistics Based on OpenFlow

DefenseFlow, through the northbound API of the SDN controller, programs the network to collect the required traffic statistic patterns from the programmable network infrastructure elements, such as openflow enabled physical and virtual switches, routers and NICs. The statistics are then sent on to the DefenseFlow application.

The statistics are used to build normal traffic baselines (stored as historical data) and continuously compare real-time traffic statistics against the pre-established baselines in order to identify abnormal patterns that may indicate DDoS attacks.

The inherent advantage of interfacing with the SDN controller is the programmability nature of the SDN infrastructure layer which allows the dynamic transformation of any network entity into a probe on demand. Changes introduced to the network such as adding switches or virtual networks are automatically discovered and mapped by the SDN controller with no need to reconfigure the DefenseFlow SDN application. It also saves the costs involved with installing and maintaining physical network probes to collect Netflow statistics per each network segment.

Analyze: Adaptive Multi-Dimension Decision Engine

DefenseFlow deploys a behavioral detection engine that is based on an adaptive fuzzy logic inference system. The system uses the following vectors to determine a degree of attack:

- Rate-based behavioral parameters such as packet rate (PPS), bandwidth (Mbps), connection rate (CPS) and more.
- Rate-invariant behavioral parameters such as protocol breakdown, average packet size distributions, connections distribution and more.
- 3rd party alerts and logs that raise suspicion of attack attempts against protected entities in the network

Unlike traditional DDoS attack detection solutions that are pure rate-based (and therefore highly prone to false-positives and false-negatives), DefenseFlow decision engine correlates between both rate based and rate-invariant parameters to determine the degree of attack. A flash crowd traffic case will result in abnormal rate-based values; however the rate-invariant parameters such as traffic distribution will remain normal – thus no attack detection is triggered.

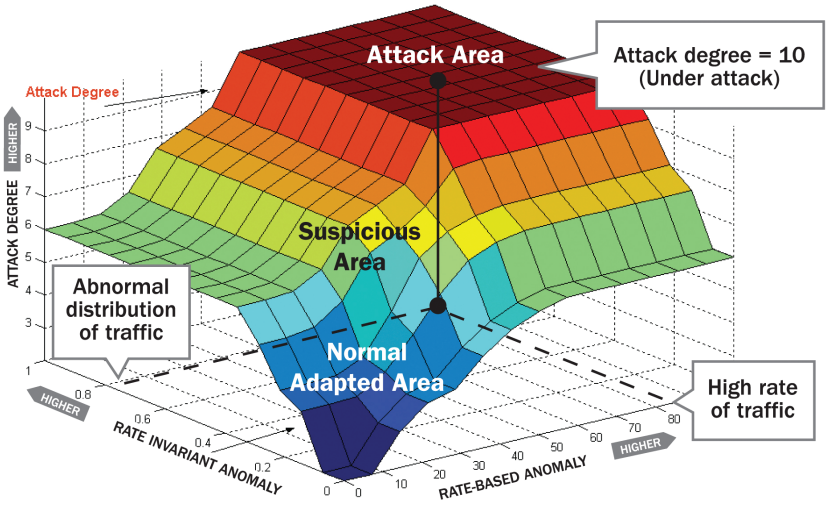


Figure 2 - The decision engine uses inputs of both rate-based and rate-invariant parameters to provide the degree of attack (or anomaly).

The power of the adaptive decision engine is that it can accurately differentiate between flash crowd traffic cases and real DDoS attacks in any network environment.

Control: Flexible Traffic Diversion Options

Once an attack is detected, the DefenseFlow programs the network through the SDN controller to divert the suspicious traffic flows through Radware's attack mitigation device (DefensePro). DefenseFlow uses the controllers northbound API to reroute traffic flows destined to the protected object under attack through the mitigation device (DefensePro). DefensePro performs attack cleansing and will then forward the clean traffic to the protected object.
The diversion mechanism is capable of decision making that includes:

- Identify the most available mitigation resource in the network
- Divert only traffic flows that are identified as suspicious
- Divert traffic back to the original path once the attack ends

The diversion engine supports automatic or manual diversion modes. The manual mode includes user-based confirmation before diversion.

As opposed to legacy network diversion approaches, DefenseFlow diversion engine provides a real-time response to attacks, with minimal network disruption, as only suspicious flows are diverted.

Management and Monitoring

DefenseFlow configuration management and monitoring are performed through a web-based management interface. Additionally, DefenseFlow extends a RESTful API to allow it to better integrate into an automated infrastructure.
Configuration management for the following parameters:

- DefenseFlow networking parameters configuration
- Protection policies and mitigation profiles
- Traffic diversion modes
- Protected networks
- Traffic learning characteristics
- Actions when attack is detected

DefenseFlow monitoring provides consolidated detailed logs and reports (of both DefenseFlow application and DefensePro mitigation device) including:

- Real-time traffic measurement of the protected objects
- Normal traffic baseline - average values of traffic per protected object
- Attack logs - identifies attack start, ongoing and end; attack information and time
- Traffic diversion state
- Real-time traffic measurements of the diverted traffic through the mitigation resources – incoming, outgoing, attack and clean traffic

Attack Mitigation with Radware DefensePro

DefenseFlow SDN application uses Radware's DefensePro as the attack mitigation resource(s).

Radware's award-winning DefensePro® is the leading DDoS protection solution in the industry, capable of mitigating all type of DoS attacks in no time.

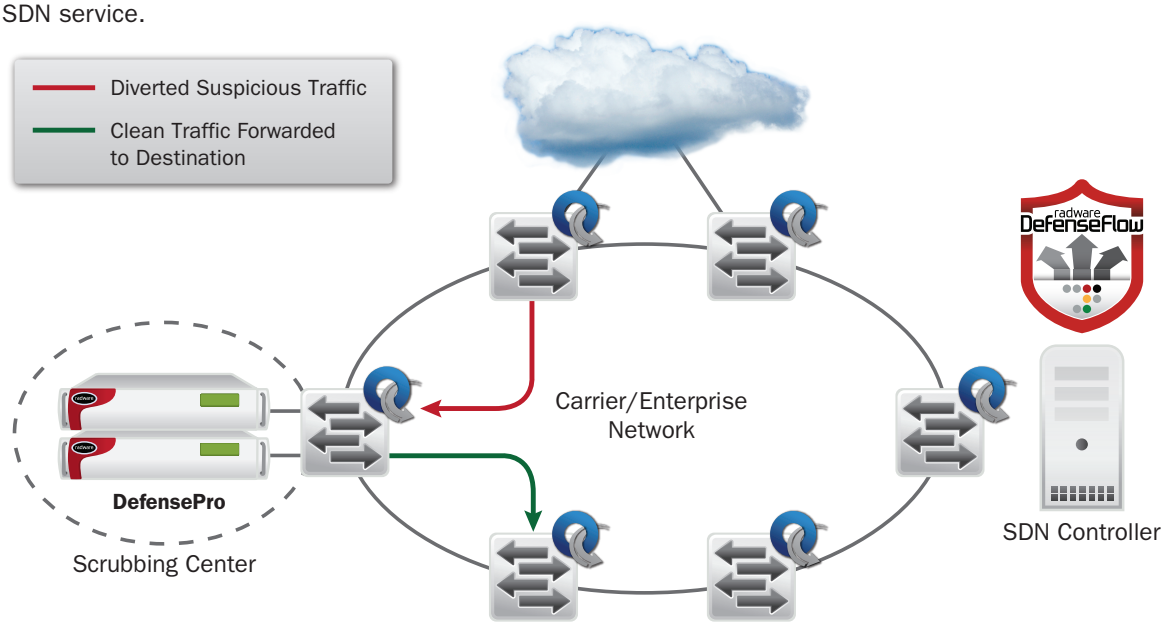
The core of DefensePro is patent protected behavioral based real-time signatures technology that detects and mitigates zero-minute DoS/DDoS attacks without the need for human intervention and without blocking legitimate user traffic.

DefensePro uses a dedicated hardware platform based on Radware's OnDemand Switch supporting network throughputs up to 40Gbps. It embeds a unique dedicated hardware component, DoS Mitigation Engine (DME), to prevent high volume DoS/DDoS flood attacks - without impacting legitimate traffic forwarding.

Use Cases

1. Multi-site scrubbing center (MSSP model)

Carrier networks or multi-site enterprises deploy network DDoS protection as a network service with separate planes for attack detection and mitigation. Using OpenFlow enabled switches/routers at the network core allows the addition of DefenseFlow to collect network statistics from all network locations while the mitigation is performed out-of-path as a native SDN service.

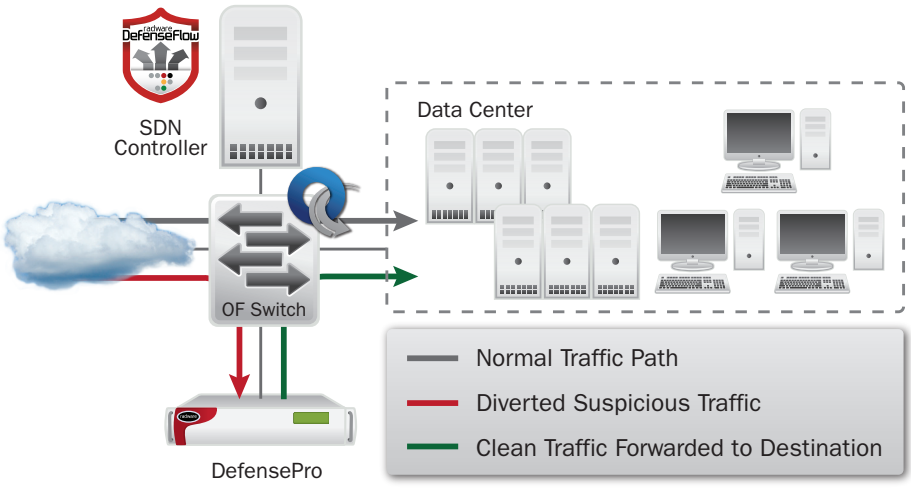


Traditionally a scrubbing center solution requires use of hardware detectors in every network location, BGP for traffic diversion and GRE tunnels to forward the traffic to its designated network object. With SDN, a DDoS protection solution gains the following advantages:

- Immediate attack detection in seconds rather than in minutes – by collecting the most relevant statistics required every few seconds.
- Low operational cost involved with traffic diversion using native SDN services instead of using tunneling (e.g. GRE, MPLS) and BGP injection.
- Overall lower solution cost: no need for multiple costly hardware detectors for every network segment due to SDN abstraction services and DefenseFlow implementation as an SDN application.

2. Local Out Of Path (LOOP)

The Local Out-Of-Path (LOOP) solution uses an OpenFlow switch (or pair for HA purposes) at the network perimeter to provide DDoS protection as a perimeter network service. The LOOP solution is applicable for data centers that have not yet implemented SDN in their network. It leverages the flexibility and programmability of SDN in order to provide a closed system, ultimately solving an existing problem. Obviously this solution can also integrate with existing SDN controllers or networks at the network edge.

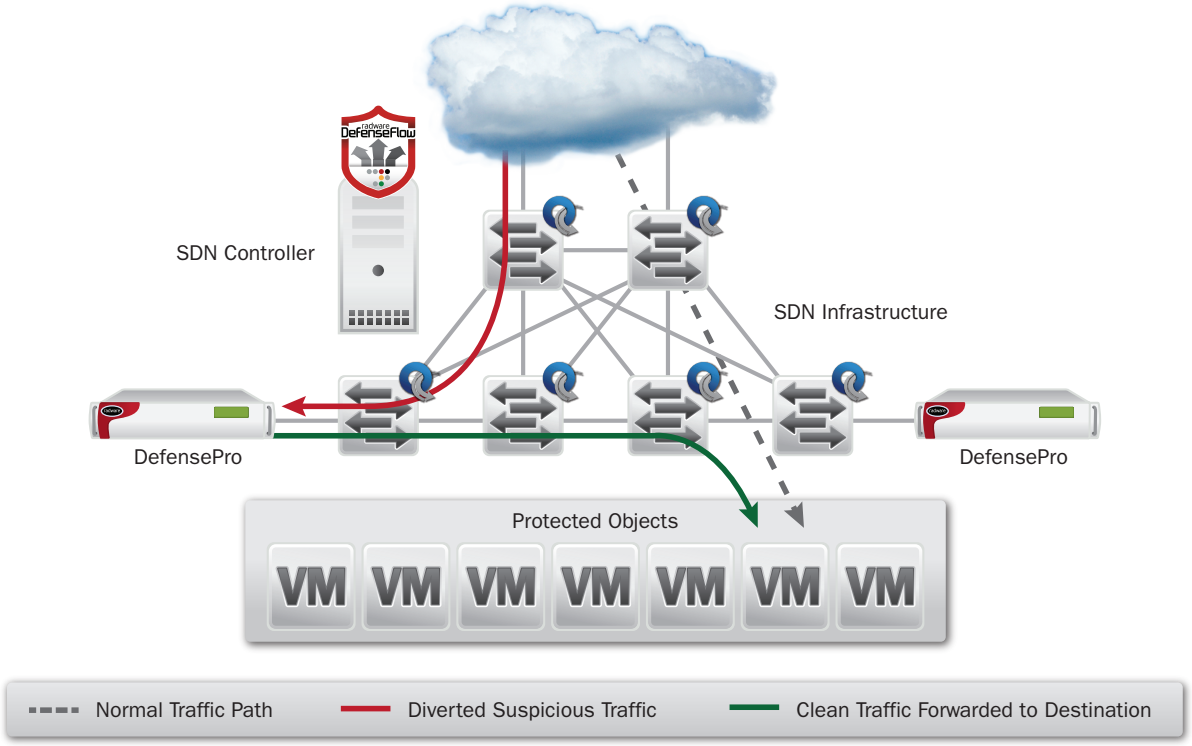


The main solution benefits are:

- Immediate attack detection in seconds rather than in minutes – by collecting the most relevant statistics required every few seconds
- Low CAPEX due to the use of low cost SDN switches
- Low false positives as traffic is diverted into mitigation device only upon attack detection

3. Full data center traffic diversion

Data centers that are moving into fully virtualized network infrastructures decouple the switching fabric from the control layer and thus can benefit from fully automated workloads and centrally control the network infrastructure. DDoS protection is deployed natively: DefenseFlow collects network statistics from switches in the data path; once an attack is detected, DefenseFlow diverts only the suspicious traffic flows to the optimal DefensePro mitigation devices in a way that best utilizes the network resources.



The result is a highly scalable and resilient DDoS protection solution implemented as a native SDN service.

Solution Benefits

Built as a native SDN application, Radware's DefenseFlow equips network operators with the following key advantages when adding DDoS protection into their infrastructure:

- Unprecedented coverage against all type of network DDoS attacks
- Best design for attack mitigation –
  - o Attack detection is always performed out of path
  - o During attack period only suspicious traffic is diverted through the mitigation device
- Most scalable mitigation solution – DefensePro mitigation devices can be placed in any location, DefenseFlow diverts the traffic to the nearest mitigation device.

Legacy DDoS protection solutions that make use of scrubbing centers are costly: need hardware detectors in every network location; BGP for traffic diversion; and GRE tunnels to forward the traffic to its designated network object. With SDN, a DDoS protection solution turns into a software application that adds intelligence to the network – no need for additional hardware, BGP or GRE operations. This is a great cost reduction opportunity for operators.

About Radware

Radware (NASDAQ: RDWR), is a global leader of application delivery and application security solutions for virtual and cloud data centers. Its award-winning solutions portfolio delivers full resilience for business-critical applications, maximum IT efficiency, and complete business agility. Radware's solutions empower more than 10,000 enterprise and carrier customers worldwide to adapt to market challenges quickly, maintain business continuity and achieve maximum productivity while keeping costs down. For more information, please visit www.radware.com.

Radware encourages you to join our community and follow us on LinkedIn, Radware Blog, Twitter, YouTube and the Radware Connect app for iPhone® .

Certainty Support

Radware offers technical support for all of its products through the Certainty Support Program. Each level of the Certainty Support Program consists of four elements: phone support, software updates, hardware maintenance, and on-site support. Radware also has dedicated engineering staff that can assist customers on a professional services basis for advanced project deployments.

Learn More

To learn more about how Radware's integrated application delivery & security solutions can enable you to get the most of your business and IT investments, email us at info@radware.com or go to www.radware.com.