radware

DefenseFlow Data Sheet

More organizations are relying on service providers to provide the infrastructure for their mission-critical applications. For the provider, this business model requires an infrastructure which is shared between different locations and across multiple tenants, thereby increasing its complexity in order to meet the needs of the customer. Unfortunately, this architecture also introduces an increase in network security threats – threats that have evolved in volume, complexity and duration, and that now present challenges to organizations trying to protect their infrastructure and customers.

In order to handle multiple services, tenants or network elements with minimal effort and still maintain a reasonable cost structure, Radware's DefenseFlow employs algorithmic capabilities that enable the automation of common NOC/SOC operations within cyber-attack mitigation workflows. These include provisioning of new services, mitigation activation, traffic diversion and attack termination. DefenseFlow enables service providers to handle large amounts of customers efficiently and with minimal errors.

The Radware DefenseFlow Solution

DefenseFlow allows service providers to easily automate security incident response operations even in the most complex and highly distributed environments. DefenseFlow cyber command and control application maximizes security effectiveness with minimal operational effort and overhead. DefenseFlow extends Radware's Attack Mitigation Solution by adding always-on/SmarTap and hosted customer protection use cases for service providers to provide the widest attack detection coverage coupled with immediate attack mitigation.

DefenseFlow Features

Radware's approach to addressing the challenges facing service providers is the Attack Mitigation Network, which involves three main components:

- **Distributed Detection** is the ability to detect a single threat across the entire network utilizing dedicated security probes, existing network elements and additional 3rd party security components. Detection capabilities include both infrastructure and application DDoS threats utilizing Layer 4-7 inline/Smartap solution.
- **Distributed Mitigation** is the ability to mitigate attacks at the optimal location utilizing different mitigation components. In this context, optimal means the furthest away from the protected infrastructure with the least disruption of traffic flow and effect on user experience. Mitigation capabilities include usage of the network as the mitigation tier, with enforcing of black hole policies by BGP flow spec, and Radware's cloud mitigation solution.
- **Centralized Control** is the facilitator of the distributed Attack Mitigation Network. It is able to collect input from Distributed Detection elements and then aggregates, correlates and analyzes in the context of the protected service. It also implements security, availability and scale logic, and applies the optimal action based on the available Distributed Mitigation components.

The Challenge

Cyber assaults against the networks of service providers can include multiple vectors with very different characteristics, thereby threatening network infrastructure elements and requiring multiple methods of mitigation.

The Solution

DefenseFlow is a network detection and cyber control application designed to detect and mitigate network-wide, multi-vector attacks. Radware's DefenseFlow supports always-on/SmarTap and hosted customer protection use cases for service providers to provide the widest attack detection coverage coupled with immediate attack mitigation.

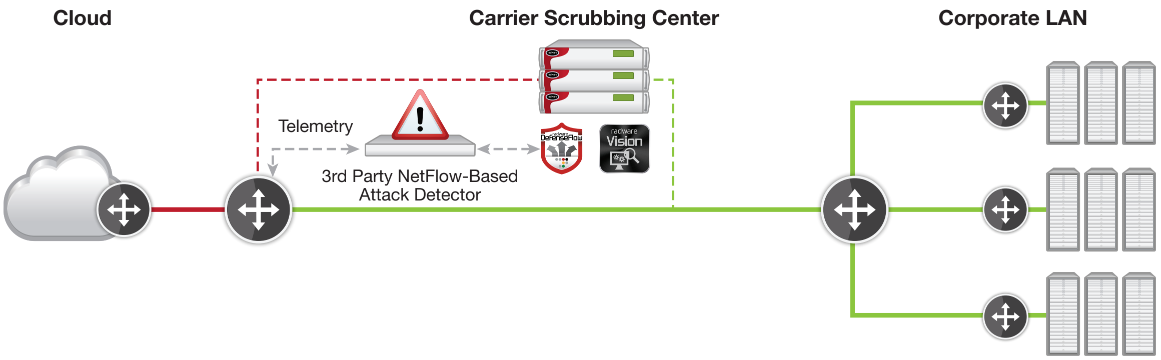
Benefits

- **Flexible use cases**, including infrastructure protection and application DDOS protection
- **Attack life cycle management**, including provisioning, attack detection, attack mitigation, and attack termination
- **Fully automated incident response** - DefenseFlow features a user friendly interface that enables operators to define actionable operations per security incident

DefenseFlow offers five use cases:

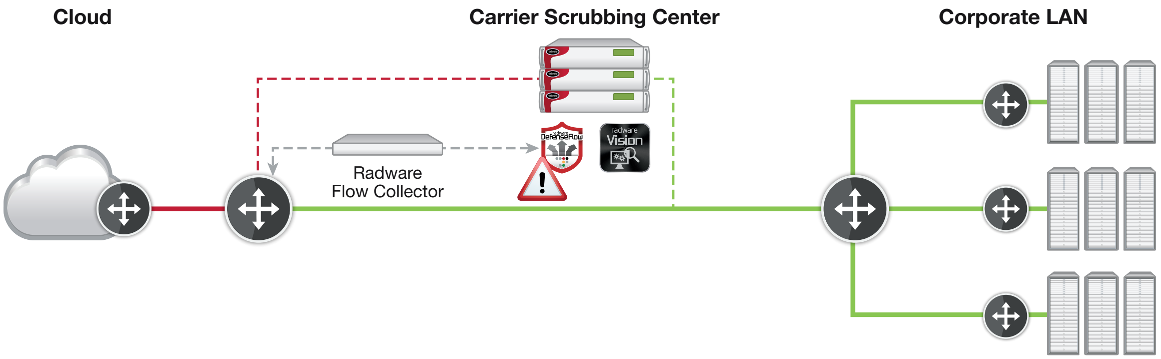
- **Use case 1**: DefenseFlow attack life cycle control with 3rd-party NetFlow attack detector (e.g. Arbor PeakFlow SP)

  In use case 1, Flow-based (Netflow) telemetry is used to detect network layer attacks from peering edges while high capacity Mitigation Center is used to protect infrastructure. In this use case the attack detection is done by a 3rd party device, usually a rate-based technologies that is coarse and prone to high false positives.



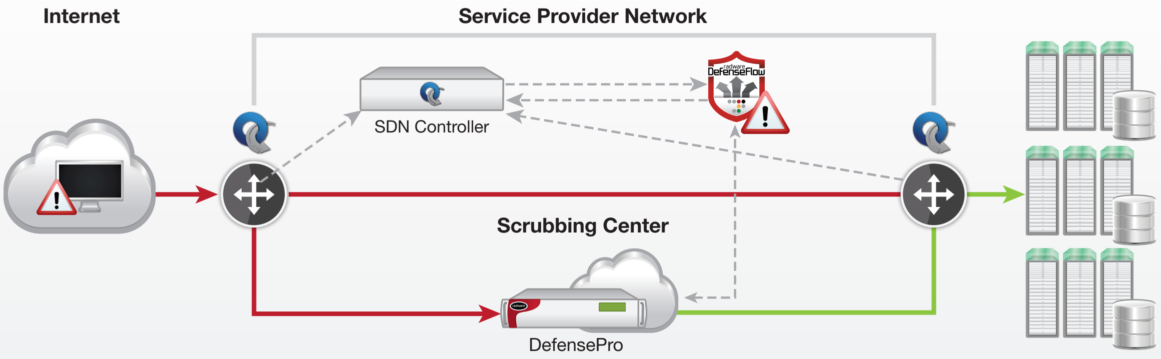
- **Use case 2**: DefenseFlow behavioral attack detection with Radware Flow Collector

  Use case 2 improves on use case 1 by offering DefenseFlow's patent-protected behavioral NetFlow based attack detection engine. While the Netflow collection is done by the Radware Netflow Collector, the attack detection is performed by DefenseFlow.



- **Use case 3**: DefenseFlow behavioral attack detection using SDN-based detection

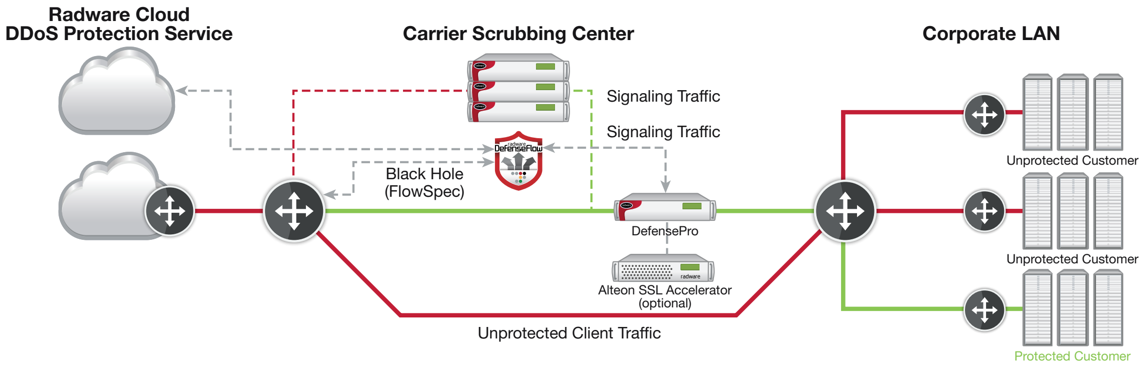
  In use case 3, DefenseFlow detects the attack via SDN Controller, configures DefensePro for attack information and traffic diversion, and finally diverts suspicious traffic for attack cleansing.



- **Use case 4**: DefenseFlow attack life cycle control with DefensePro as attack detector

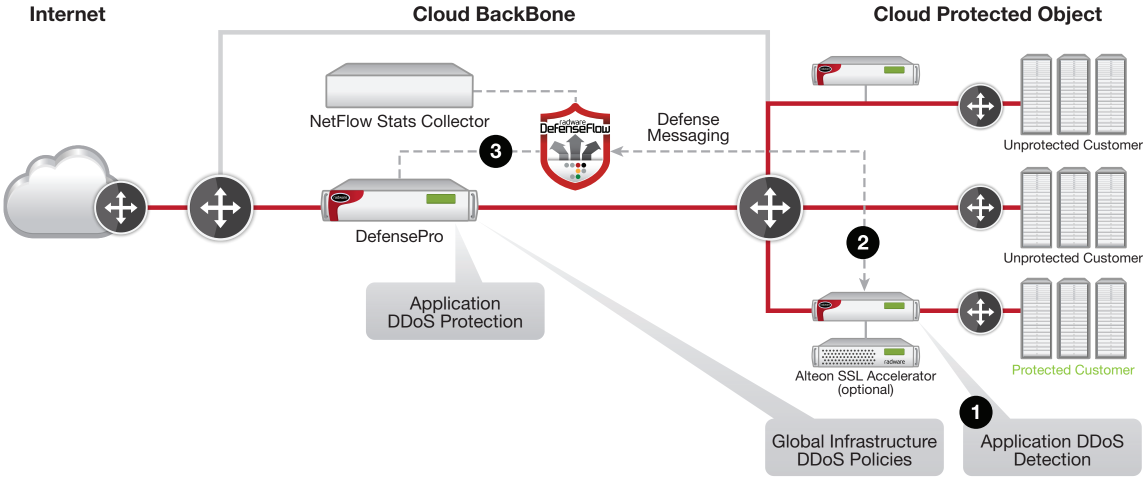
  In this use case, data center applications are protected by advanced inline / SmarTap detection with signaling to activate higher tier mitigation when necessary. DefensePro can be installed as customer-premise equipment

(CPE). Additionally, DefesePro to DefensePro delegation offers the ability to copy DefensePro configuration and baseline information between mitigation tiers, e.g. CPE, Scrubbing Center, and Cloud. This capability allows immediate mitigation without additional learning and detection time.



- **Use case 5**: DefenseFlow attack life cycle control with DefensePro or NetFlow detection (Hosting)

  Lastly, hosting providers' customers may be protected by using DefensePro to protect cloud-based protected objects. This is achieved by providing common security policies for all protected objects, and (using SmartTap), detecting application attacks, utilizing defense messaging, and mitigating the attack on the cloud backbone. In this case, the scrubbing center DefensePro will mitigate the high vulnerability attacks.



DefenseFlow Benefits Summary

Use Case	Attack Detection Method	Operation	Benefits
1	**3rd-Party Netflow-based Detector**	Traffic diversion to scrubbing center using BGP	- Best quality-of-mitigation solution in the industry - Widest attack coverage, mitigating all types of DoS/DDoS attacks - Highest mitigation accuracy, blocks attack traffic without blocking legitimate user traffic - Saves on SOC costs involved with handling attack leakage and false positives
2	**DefenseFlow behavioral analysis engine with NetFlow telemetry**	Traffic diversion to scrubbing center using BGP	Use Case 1 benefits plus: - Best quality-of-detection solution with DefenseFlow's patent-protected behavioral NetFlow/OpenFlow based attack detection - The lowest false detection rate in the industry with attacks detection in seconds

3	**DefenseFlow behavioral analysis engine with OpenFlow telemetry**	Traffic diversion to scrubbing center using SDN	Use cases 1 + 2 plus: - Immediate attack mitigation by using SDN-based traffic diversion
4	**DefensePro**	- Local mitigation with DefensePro - Traffic Diversion to scrubbing center using BGP-FS - Inject mitigation policy to peering DefensePro - Shared mitigation policy between mitigation devices - Set black holing rule on Peering router	Use cases 1 + 2 plus: - Immediate attack mitigation with all attacks mitigated on-premise by DefensePro - Flexible operations per incident type, resolving any service provider use case
5	• **DefensePro** • **DefenseFlow behavioral analysis engine with NetFlow telemetry**	Inject mitigation policy to peering DefensePro	Use cases 1 + 2 plus: - Granular per-tenant attack detection, protecting hosting provider customers against lower volume DDoS attacks that would normally go undetected

Summary

DefenseFlow allows service providers to easily automate security incident response operations even in the most complex and highly distributed environments. The cyber command and control application maximizes security effectiveness with minimal operational effort and overhead. DefenseFlow extends Radware attack mitigation solution by adding always-on/SmarTap and hosted customer protection use cases for service providers to provide the widest attack detection coverage coupled with immediate attack mitigation.

About Radware

Radware® (NASDAQ: RDWR), is a global leader of application delivery and cyber security solutions for virtual, cloud and software defined data centers. Its award-winning solutions portfolio delivers service level assurance for business-critical applications, while maximizing IT efficiency. 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: Facebook, Google+, LinkedIn, Radware Blog, SlideShare, Twitter, YouTube, Radware Connect app for iPhone® and our security center DDoSWarriors.com that provides a comprehensive analysis on DDoS attack tools, trends and threats.

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.

This document is provided for information purposes only. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law. Radware specifically disclaims any liability with respect to this document and no contractual obligations are formed either directly or indirectly by this document. The technologies, functionalities, services, or processes described herein are subject to change without notice.