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 that 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 infrastructures 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 which enable the automation of common NOC/SOC operations within cyberattack 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. The 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/SmartTap and hosted customer protection use cases for service providers to provide the widest attack detection coverage coupled with immediate attack mitigation.

Distributed Protection

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 by utilizing dedicated security and network elements and additional third-party security components. Detection capabilities include both infrastructure and application DDoS threats by utilizing the Layer 4–7 in-line/SmartTap solution.

- **Distributed Mitigation** is the ability to mitigate attacks at the optimal location by 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 enforcement of black hole policies by border gateway protocol (BGP) flow specification (flowspec), 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 it 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

Cyberassaults 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 cybercontrol application designed to automate and orchestrate the detection and mitigation of network, multivector attacks. Radware's DefenseFlow supports always-on/SmartTap and hosted customer protection use cases for service providers to provide the widest attack detection combined with real-time 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

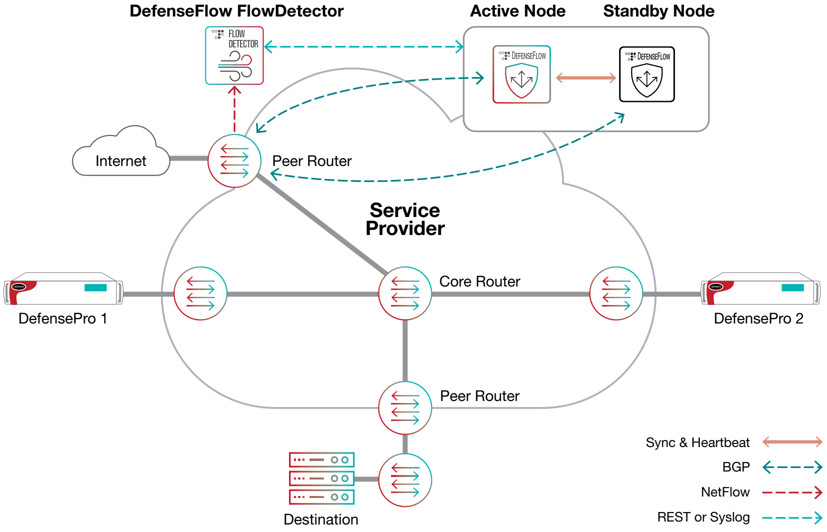
- Fully automated incident response — DefenseFlow features a user-friendly interface that enables operators to define actionable operations per security incident

Ensuring High Availability

DefenseFlow high availability increases system stability and enables service accessibility through elimination of a single point of failure. When a component fails, DefenseFlow recovers automatically.

In the DefenseFlow high-availability architecture, there are two identical DefenseFlow nodes: active and standby. Both nodes communicate with each other and maintain full synchronization for both component state and configuration.

DefenseFlow creates a peer from each active/standby node to each router, resulting in two peer connections for each network element. If one node fails, the other node keeps the peer connections and the related announcements active.



When a DefenseFlow node fails, the remaining node continues to communicate with all registered routers and third-party detectors with zero downtime.

Attack Dashboard Provides Visibility and Control

Radware provides a full attack dashboard to simplify the user experience and reduce customer opex. The dashboard enables the customer to easily monitor and operate DefenseFlow.

The dashboard provides a single view of all incoming attacks and ongoing active protections, as well as a complete history of all the attacks and protections handled by the system. It gives the user flexibility in taking action, such as the ability to manually activate/deactivate single or multiple protections with a single click or manually add/remove networks/classless interdomain routing from an ongoing protection.

Flexibility with Customized Operations

DefenseFlow is able to activate and deactivate various types of predefined operations once a workflow rule entry and exit criteria are matched. As part of the set of predefined operations, DefenseFlow can divert and block traffic based on a BGP or a flowspec rule. DefenseFlow can also deploy different types of policies and profiles on one or a group of mitigation devices.

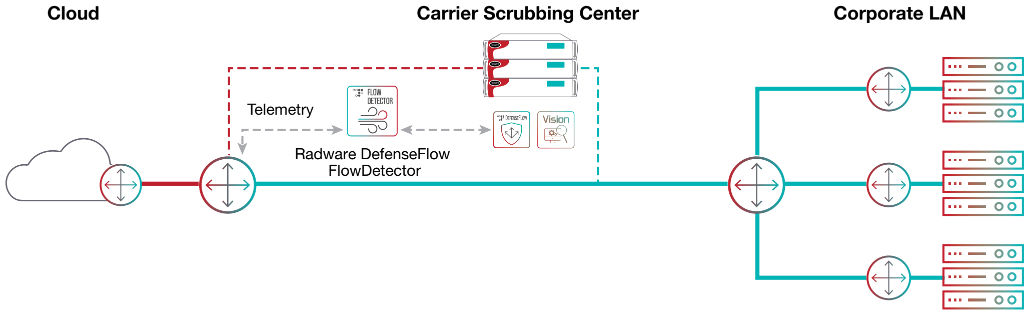
DefenseFlow also enables the customer to define and program its own customized operation to match the unique needs of its network. DefenseFlow ensures that the new customized operation is activated whenever a protection is required in accordance to a rule criteria match within its workflow engine.

DefenseFlow Use Cases

DefenseFlow offers three use cases:

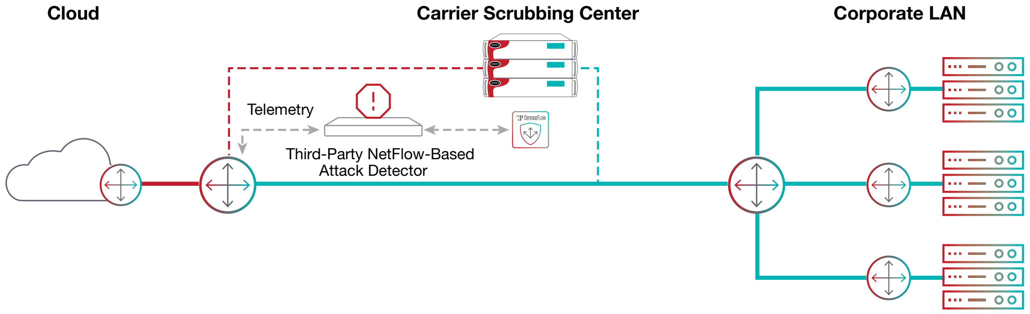
- **Use case 1:** DefenseFlow attack life cycle control with Radware's DefenseFlow FlowDetector

  In use case 1, flow-based telemetry is used to detect network-layer attacks from peering edges while a high-capacity mitigation center is used to protect the infrastructure. In this use case, the attack detection is done by DefenseFlow FlowDetector for centralized management, control and support.



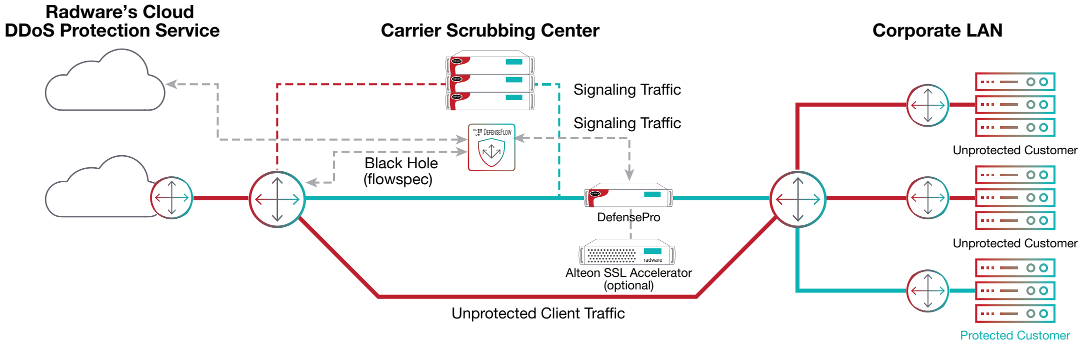
- **Use case 2:** DefenseFlow and third-party flow telemetry detector

  This use case leverages the same architecture logic but with the incorporation of third-party flow telemetry devices (such as Nokia, Arbor and Flowmon).



- **Use case 3:** DefenseFlow attack life cycle control with DefensePro as attack detector.

  In this use case, data center applications are protected by advanced in-line/SmartTap detection with signaling to activate higher tier mitigation when necessary. DefensePro can be installed as customer-premise equipment (CPE). Additionally 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.



DefenseFlow Benefits Summary

Use Case	Attack Detection Method	Operation	Benefits
1	**Radware's DefenseFlow FlowDetector**	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 - Single pane of glass - Single vendor solution
2	**Third-party NetFlow-based detector**	Traffic diversion to scrubbing center using BGP	Best mitigation solution in the industry - Wide attack coverage for mitigation of all types of DoS/DDoS attacks - Highest mitigation accuracy to block attack traffic without impacting legitimate user traffic
3	**DefensePro**	Local mitigation with DefensePro - Traffic diversion to scrubbing center using BGP flowspec - Inject mitigation policy to peering DefensePro - Shared mitigation policy between mitigation devices - Set blackholing rule on peering router	Use case 1 plus: - On-premise attack mitigation by DefensePro - Flexible operations per incident to resolve any service provider use case - Application-layer protection - Low and slow attack protection

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's Attack Mitigation Solution by adding always-on/SmartTap 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 cybersecurity and application delivery solutions for physical, cloud and software-defined data centers. Its award-winning solutions portfolio secures the digital experience by providing infrastructure, application and corporate IT protection and availability services to enterprises globally. Radware's solutions empower more than 12,500 enterprise and carrier customers worldwide to adapt quickly to market challenges, 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: Radware Blog, LinkedIn, Facebook, Twitter, YouTube, Radware Connect app for iPhone® and our security center DDoSWarriors.com that provides a comprehensive analysis of DDoS attack tools, trends and threats.