DefenseFlow – SDN Based Network DDoS, Application DoS and APT Protection

Radware's DefenseFlow SDN application allows organizations to dynamically mitigate Network, Application and APT attacks utilizing the entire network capacity.

Challenge

Organizations are struggling to keep up with the evolving information security threat landscape. Protection against evolving threats of unknown nature and magnitude is something organizations are not geared to handle. The dynamic nature of evolving threats increases organizational risk, drains organizational resources on the operations side and find existing security protections useless.

Solution

Radware offers dynamic attack mitigation solutions that mitigate network DDoS, Application DDoS and Advanced Persistent Threats. By cooperatively operating with software defined networks, and leveraging the programmable and dynamic nature of SDN, Radware DefenseFlow is the only solution that can economically and effectively counter the dynamic nature of emerging threats.

Benefits

- A scalable Attack Mitigation solution leveraging the entire SDN capacity.
- Address Network DDoS, Application DDoS and APT security threats.
- Economical Attack Mitigation Solution optimally utilizing general purpose network resources and purpose built software.
- Ideal for large scale datacenters, campus networks and service provider networks.

New security threats to telecommunications providers and enterprises require rapid provisioning of security protection solutions capable of identifying and blocking unknown attacks at unknown scale. Radware DefenseFlow is an SDN Based Adaptive Attack Mitigation solution offering the ability to dramatically accelerate security capability provisioning time while automatically integrating into diverse and large scale networks.

The Challenge

As applications and information systems are increasingly critical elements of businesses – such to which outages present significant adverse impact on the bottom line of business operations, Applications and network infrastructures are required to continuously operate under any attack circumstance by offering adequate level of protection from any given threat. However a few common assumptions that were regularly used when implementing information security systems are no longer true as follows:

Since workloads in the modern datacenter regularly move, the physical placement of a particular business application can no longer signify its logical role and help in categorizing risk related parameters associated with objects.

The dynamic nature of compute workloads highlight that the need to redesign networks in order to mitigate unknown and emerging threats and risk is no longer acceptable. Additionally, redesigning networks per attack takes too long and is insufficient when only immediate response to attacks will support required business continuity.

Beyond workload mobility, applications often scale-out to address variable demand. Therefore, applications become a moving target causing targeted application attacks to impact large sets of infrastructure elements. The magnitude of this impact leads to greater and often unmanageable risk levels that businesses are not willing to take.

Ultimately, the longer time associated with provisioning security protections against the described threats, increases the risk due to the described potential outages. Current static security measures do not offer the proper level of protection against unknown, dynamic, large scale threats.

The DefenseFlow Solution

DefenseFlow uniquely addresses the new requirements by leveraging the programmable and dynamic nature of software defined networks and by employing adaptive security algorithms combining the following capabilities:

(1) Uniquely identify network level, application level & APT attacks,
(2) Instantaneously provision security capabilities throughout the network and
(3) Distribute the attack mitigation functionality leveraging the entire SDN capacity.

While alternative approaches require static provisioning of security systems throughout the network and sized according to the protected network capacity, DefenseFlow leverages the entire network combined with on-demand intelligence of network, application and APT recognition algorithms, by using only the exact amount of resources needed, at the optimal network location in order to identify and block various attacks at various sizes.

The solution operates using a continuous 4 stage service lifecycle:

1. **Provision** Security detection throughout the network by programming counters throughout the SDN nodes, by provisioning L4-7 Application Intelligence (AI) engines & by mirroring traffic to the L4-7 AI engines.
2. **Collect** information from the entire set of provisioned information sources.
3. **Analyze** network and application information in order to categorize behavioral patterns, maintain an ongoing behavioral baseline and identify any steep deviations from the baseline.
4. **Control** traffic and service elements by blocking traffic, diverting traffic to dedicated attack mitigation engines and optimizing security policies.

The solution is an evolution of the DefenseFlow Network Behavioral Analysis (NBA) solution, adding to it an Application Behavioral Analytics (ABA) Component as well as an Advanced Persistent Threat (APT) Detection Module. In order to formulate a consistent and actionable behavioral baseline, and identify deviations from this baseline at the application behavior and APT levels, several implementations of patented behavioral analysis mechanisms are used. These mechanisms define real-time application and network attack signatures most effective against modern zero-day attacks. Furthermore, the ability to scale intelligent application level attack detection engines on the fly and distribute traffic across these engines intelligently (leveraging SDN) is pending patent under the Radware ElasticScale network services framework.

The illustration outlines various capabilities of the DefenseFlow solution by showing the following elements:

- User & Server networks, these are organizationally controlled assets under which the SDN is assumed to operate (fully or partially) for collecting traffic statistics, mirroring traffic to vDPI engines & blocking traffic.
- Edge network through which all traffic in and out of the organization passes; this network section is assumed to be fully SDN capable and is responsible for collecting traffic statistics, mirroring traffic to vDPI engines, diverting Traffic to Attack Mitigation systems & blocking traffic.
- The L4-7 Service fabric which is pictured as a single area, but can be distributed throughout the entire SDN as best suited to protect the network. The fabric consists of L4-7 systems such as DPI engines, attack mitigation systems etc. the DPI engines are responsible to collect Application layer meta-data and statistics and the Attack mitigation systems are responsible to block attacks at very high certainty.
- The solution control plane consists of the SDN controller and DefenseFlow applications and is responsible for programming the network to: collect network statistics, intelligently mirror traffic to vDPI elements, Divert suspicious traffic to Attack mitigation systems and block malicious traffic at most appropriate network locations.

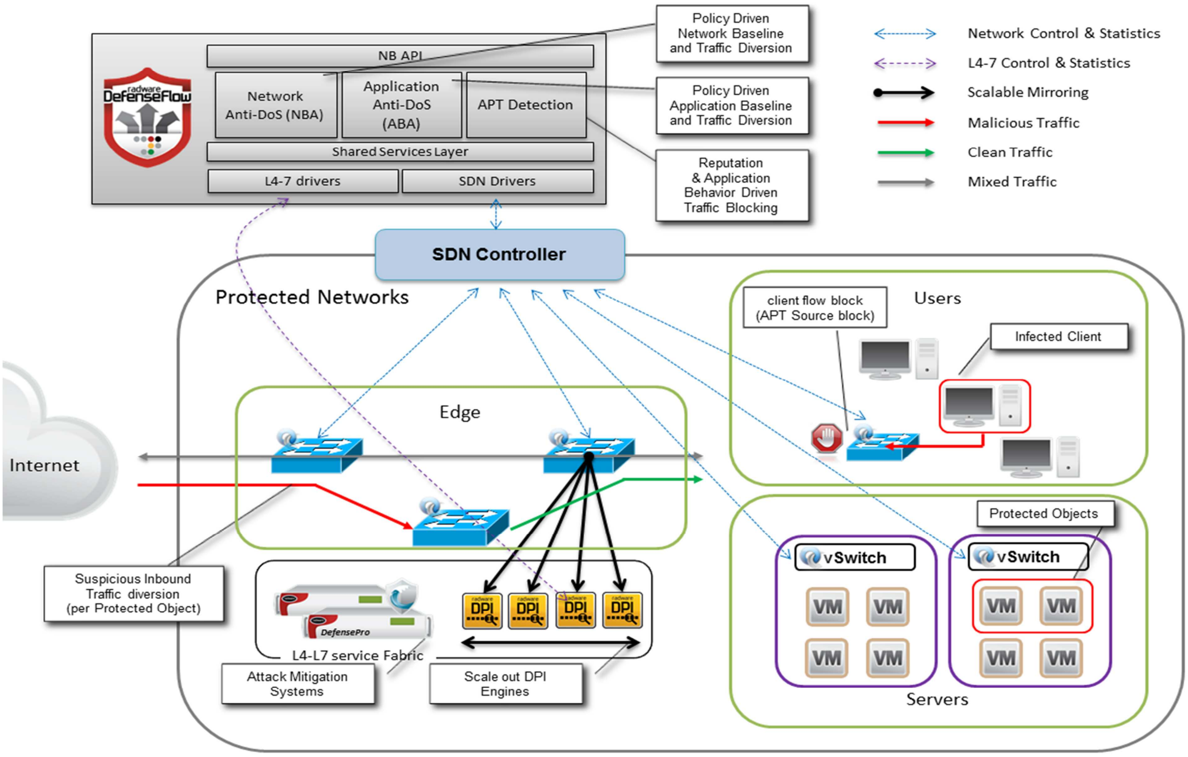
NB API
DefenseFlow
Network Anti-DoS (NBA)
Application Anti-DoS (ABA)
APT Detection
Shared Services Layer
L4-7 drivers
SDN Drivers
Policy Driven Network Baseline and Traffic Diversion
Policy Driven Application Baseline and Traffic Diversion
Reputation & Application Behavior Driven Traffic Blocking
Network Control & Statistics
L4-7 Control & Statistics
Scalable Mirroring
Malicious Traffic
Clean Traffic
Mixed Traffic
SDN Controller
Protected Networks
Edge
Internet
client flow block (APT Source block)
Users
Infected Client
Protected Objects
vSwitch
vSwitch
VM
Servers
Suspicious Inbound Traffic diversion (per Protected Object)
DefensePro
DPI
L4-L7 service Fabric
Attack Mitigation Systems
Scale out DPI Engines

Figure 1 – DefenseFlow – Distributed Attack Detection, Traffic Diversion & Attack Mitigation

Features and Benefits

- Ultra scalable Attack Mitigation solution (100's of Gbps)
- Very Fast Zero Day Attack Detection and Mitigation
- Based on industry leading, Field Proven Security Behavioral Analysis Algorithms
- Selective Security policy driven protection against network and application DoS attacks
- Compatible with leading SDN controllers; OpenDaylight, Cisco APIC, NEC pFlow & HP VAN
- Runs over any physical SDN network equipment

Summary

The DefenseFlow **Adaptive Network, Application and APT Protection** solution leverages the field proven Radware Attack Mitigation System mechanisms, in form of an SDN application, together with SDN to enable cost effective and scalable Attack Mitigation capabilities for organizations. The solution addresses a broad range of security threats from network DDoS through Application DDoS to APT offering organizations one of the most cost effective solutions to mitigate organizational risk.

DefenseFlow is a perfect example of how SDN changes existing network service architectures to employ a collaborative mechanism in which network and L4-7 systems interact and increase value to end user. This is done by changing the network role from hosting services - to being part of the service - in this case offering increased security protection. DefenseFlow is the only solution that addresses the dynamic nature (unknown type and scale) of Attacks and brings the dynamic capabilities of SDN to mitigate the associated risks. Furthermore, as opposed to other available solutions that offer new API's to program existing systems. DefenseFlow is a clear showcase of how SDN offers immediate value to organizations that run business critical networks.

Further Reading

For more information regarding Radware SDN solutions check out the following URL: http://www.radware.com/Solutions/SDN/