CISCO AND RADWARE: BUILD APPLICATION CENTRIC, DoS/DDoS PROTECTED DATA CENTERS

Introduction

The demand from modern IT organizations to transform the infrastructure and enable rapid application rollout while controlling application quality of service (QoE) and guaranteeing service level agreement (SLA) assurance poses new and significant challenges. Cisco's application centric approach to rolling out new network silos is a significant improvement; however, IT departments still struggle to guarantee application SLA when under attack.

Cisco Application Centric Infrastructure (ACI) provides an innovative application and security service insertion framework, with the Cisco Application Policy Infrastructure Controller (APIC) as a central point of network service automation and policy control.

Cisco APIC allows IT administrators to automate the insertion and provisioning of security services in application networks. It eliminates the complexity of traffic-steering techniques and topology constraints of traditional networks, and enables application mobility and cloud readiness.

By integrating Cisco ACI with Radware's Attack Mitigation System (AMS), IT organizations can streamline DoS/DDoS protection as a native network service. Data centers can dynamically associate security services per application and reduce the overall cost of solution, streamlining operations and improving the overall security protection against advanced DDoS attacks.

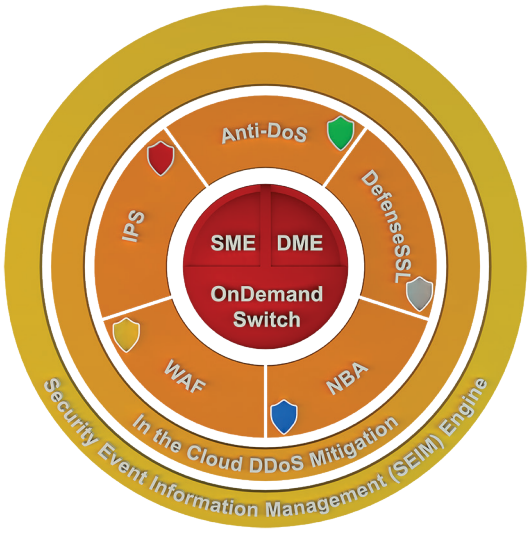
Radware Attack Mitigation System

Emerging network threats require multiple protection tools to secure a data center from network downtime, application downtime, application vulnerability, malware spread, web application attacks and web defacement. Radware AMS integrates anti-DoS, network behavioral analysis (NBA), SSL defense, intrusion prevention system (IPS) and web application firewall (WAF) in one system that is designed to protect data centers against known and emerging network and application threats.

AMS enables online businesses, data centers and service providers to assure their on-line presence and maintain productivity.

Radware AMS offers the following benefits:

- **Widest security coverage.** Detecting and mitigating all types of availability based attacks that target the application infrastructure.
- **Shortest response time.** AMS guarantees real-time detection and mitigation of network, application and low & slow attacks.
- **Top security expertise.** Radware's Emergency Response Team (ERT) composed of security experts use the most up-to-date methodologies and to empower customers to handle persistent attacks that last day or even weeks, help form new protections in real time, and deploy counterattack techniques.



Challenges

In today's data centers security solutions such as firewalls, intrusion prevention systems (IPS), web application firewalls and DDoS protection are typically installed as stand-alone solutions. The current network infrastructure is hosting security solutions, and operators are required to manually perform processes and management tasks with little or no automation.

To better align applications and data centers with business operations activity and better adapt to changing requirements, organizations need automation based predefined policies and on-demand, user-controlled updates to applications and infrastructure.

Solution Overview

The integration of the Cisco ACI architecture with AMS provides automated, policy-based security provisioning, management, and security policy updates for DoS/DDoS attacks protection services. Radware AMS and Cisco ACI provide transparent security services anywhere in the network fabric including centralized management, monitoring and reporting per application or tenant.

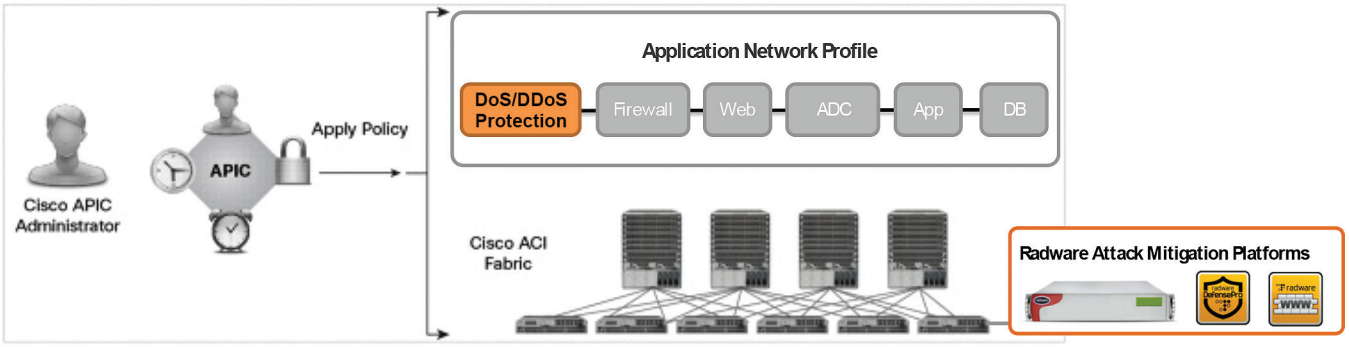


Figure 1: Radware Attack Mitigation System (AMS) and Cisco ACI

AMS devices (or virtual appliances) are connected to the network as part of Cisco ACI Fabric and controlled by Cisco APIC.

When a new application network profile is created, the user can add DoS/DDoS protection services into the service chain. Once APIC applies the new profile per application-tenant or network-tenant, the traffic is inspected by Radware AMS to maintain service availability even when the service is under attack. AMS detects attacks in real-time and dynamically modifies APIC policies removing attack traffic without blocking legitimate user traffic.

Solution Benefits

The joint Cisco and Radware solution offers the following unique benefits:

- **Application Policy Driven Security** Transparent integration with Cisco ACI data center fabric enforces consistent security anywhere in the data center, for physical and virtual workloads. Centralized management and automation through Cisco APIC simplifies the operation complexity associated with security policy enforcement and provides system-wide visibility of security-aware applications and tenants.
- **Ease of Deployment** Applications can move, scale-up or scale-out while retaining the associated services without any location specific constraints. Application policies can be optimized to best address the changing SLA requirements of applications as ACI utilizes Radware security services throughout the network.
- **Error-free Deployment** Automated processes applied by Cisco APIC running vendor-certified use cases eliminate user learning curve and staging periods, typically required for new security services provisioning and configuration.
- **Best DDoS Protection Solution** Radware's unique and field-proven DDoS protection technology and Cisco ACI provide the widest attack coverage in the industry against all types of network and application DDoS attacks that threaten the availability of the application infrastructure.

Summary

With Cisco ACI's advancements in network automation and Radware security services, organizations can meet the growing requirements to run business critical applications in the datacenter. Organizations that build their datacenter network using ACI can now guarantee application availability by adding DoS/DDoS protection services to protect against the sophisticated cyber threats.

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 Facebook, Google+, LinkedIn, Radware Blog, SlideShare, Twitter, YouTube and the Radware Connect app for iPhone®.