Cisco and Radware: Build Application-Centric Data Centers with DoS and DDoS Protection

Introduction

The demand from modern IT departments to transform the infrastructure to enable rapid application rollout while controlling the application quality of service (QoS) and meeting service-level agreements (SLAs) poses new and significant challenges. Although Cisco's application-centric approach significantly improves the capability to roll out new network services, the capability to guarantee application SLAs during denial-of-service (DoS) and distributed DoS (DDoS) attacks remains a significant challenge to IT departments.

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 physical and virtual security services in application networks, thus eliminating the complexity of traffic-steering techniques and the topology constraints of traditional networks and enabling application mobility and cloud readiness.

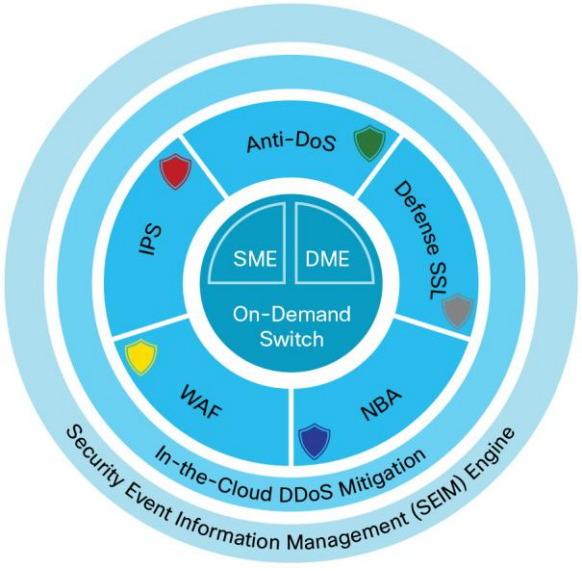
By integrating Cisco ACI with Radware Attack Mitigation System (AMS), IT departments can simplify DoS and DDoS protection by making it a native network service. This approach allows data centers to dynamically associate security services per application or per tenant while reducing the overall cost of the solution, simplifying operations, and improving overall security protection against advanced DDoS attacks.

Radware Attack Mitigation System

Emerging network threats require multiple protection tools to secure your business data center from threats such as 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) solutions in one system designed to protect data centers against known and emerging network and application threats (Figure 1).

Figure 1: Radware AMS



With Radware AMS, online businesses, data centers, and service providers can help ensure their online presence and maintain productivity.

Radware AMS offers the following benefits:

- **Wide security coverage:** AMS detects and mitigates all types of availability-based attacks targeting the application infrastructure.
- **Short response time:** AMS helps ensure real-time detection and mitigation of network, application, and low-and-slow attacks.
- **Top security expertise:** The Radware Emergency Response Team (ERT), composed of security experts using the most up-to-date methodologies and tools, empowers customers to handle persistent attacks that last days, quickly form new protection approaches in real time, and deploy counterattack techniques.

Challenges

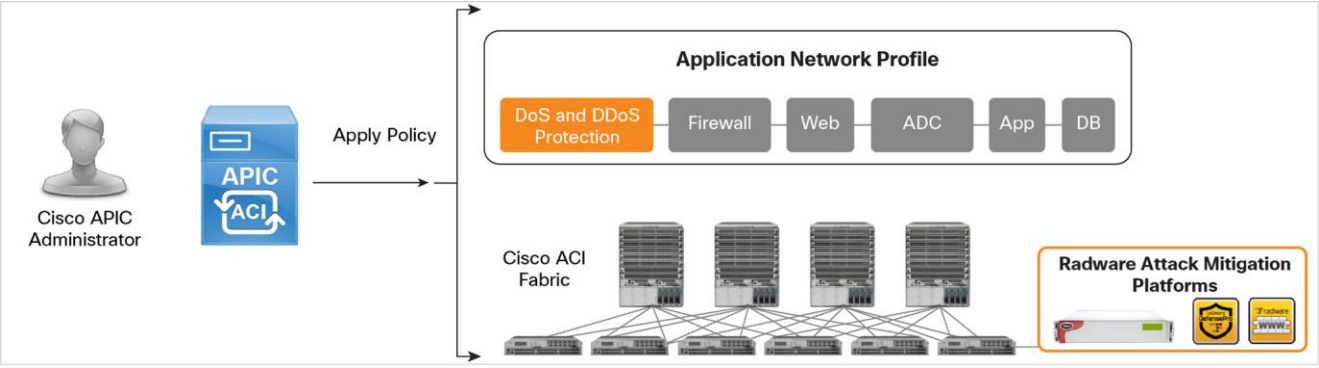
In today's data centers, security solutions such as firewalls, IPSs, web application firewalls, and DDoS protection are typically installed as standalone solutions. The current network infrastructure just hosts the security solutions, and operators are required to manually perform processes, provisioning and management tasks, with little or no automation.

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

Solution Overview

The integration of the Cisco ACI architecture with Radware AMS provides automated, policy-based security provisioning, management, and security policy updates for DoS and DDoS attack protection services. Radware AMS and Cisco ACI enable transparent security services insertion anywhere in the network fabric, centralized management and monitoring, and reporting per application or per tenant (Figure 2).

Figure 2: Radware AMS and Cisco ACI



Radware 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 and DDoS protection service to the service chain. After the APIC applies the new profile to the application tenant or network tenant, the tenant traffic is inspected by Radware AMS to maintain service availability even when the service is under attack. Radware AMS detects attacks in real-time and dynamically modifies APIC policies, thus removing attack traffic without blocking legitimate user traffic.

Solution Benefits

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

- **Application policy-based 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 systemwide visibility of security-aware applications and tenants.
- **Ease of deployment:** Applications can be moved, scaled up, or scaled 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 Cisco ACI uses Radware security services anywhere throughout the network.
- **Error-free deployment:** Automated processes applied by the APIC running vendor-certified use cases eliminate the need for user learning and staging periods typically required when new security services are provisioned and configured.
- **Excellent DDoS protection solution:** Radware's unique and field-proven DDoS protection technology together with Cisco ACI provides the widest attack coverage in the industry, protecting against all types of network and application DDoS attacks that threaten the availability of the application infrastructure.

Conclusion

With the advances in network automation becoming available with Cisco ACI and the ever-growing need to run business-critical applications on the data center network for public/hybrid/private cloud use cases, keeping the data center safe from attacks is more important than ever. With Radware security services, organizations can make the jump to ACI more safely and with a clearer path to the benefits of ACI. Organizations building their data center networks using Cisco ACI can now further increase their confidence in the availability of their applications by adding DoS and DDoS protection services as part of the application service chain, using Radware's world-leading AMS solution to protect against the world's most sophisticated cyberthreats.

For More Information

- To learn more about Cisco ACI, visit http://cisco.com/go/aci.
- To learn more about Radware, visit http://www.radware.com.

C22-733709-00 01/15