FORTIADC CONNECTOR FOR CISCO ACI
Unified Application Policy and Orchestration

Software-defined application delivery provides the agility and high availability needed in a workload-driven data center, so IT can respond quickly to changing business requirements. Evolving applications in the cloud now ask for on-demand and 13x9s always-on reliability, which is highly dependent on the infrastructure they are running on. By providing an orchestration, abstraction, and transparent infrastructure for application deployment, data-center operators can have the control and visibility to manage and address application delivery policies as new workloads are introduced. Existing data centers and private cloud environments generally have a mixture of physical and virtual appliances, which come from various appliance vendors. To avoid time-consuming policy control silos and manual hair-pinning rulesets, modern IT needs a new process to deploy and scale applications quickly.

Cisco Application Centric Infrastructure (ACI) offers the software-defined platform for Layer 4-7 service function automation and policy management framework. Data-center IT can use Cisco Application Policy Infrastructure Controller (APIC) as the enforcement point for application policies to configure application-specific network requirements. FortiADC Connector for Cisco ACI is an XML device package that serves as a plugin running on APIC directly. IT can configure the FortiADC without actually touching the physical or virtual appliance. By exposing L4 service functions of FortiADC, the joint solution offers a single point of efficient application delivery automation and management.

SOLUTIONS HIGHLIGHTS

- Automates Layer 4 application service insertion, policy updates, and optimization within the ACI-enabled fabric with FortiADC
- Seamlessly integrates topologies in FortiADC physical and virtual appliances
- Reduces operating spending on provisioning application workflows through consistent policy-driven delivery
- Supports Fortinet’s patented virtual domains across multiple tenants
The joint solution helps transform the data center to adapt effectively with application-centric workloads and significantly improves application provisioning and agility. The architecture provides a common management framework for network, application, security, and virtualization teams, making IT more agile while reducing application deployment time.

**In Cisco ACI, network segmentation and security policies are enforced consistently whenever a new application is deployed in the network. This joint solution supports Go-To (Transparent) and Go-Through modes.**

**Go-Through Mode (Layer 2)**

Devices in Go-Through or Transparent mode are considered Layer 2 devices to affect traffic. These devices are not referred to by the packet’s destination MAC or IP address. In most cases, these devices will only have an address for the purposes of management.

**Go-To Mode (Layer 3)**

This support helps route traffic and references the destination in a packet’s destination MAC address or destination IP address.

**Multitenant, Multidevice Support**

- Multitenant and multidevice are typical in the use cases of FortiADC integration with Cisco ACI. When the FortiADC device is added, a tenant's L4 services and multicontext aware can be enabled. This indicates to the device package that the L4 device is going to be a virtual device that shares resources with other tenants on the FortiADC. In FortiADC implementation, this virtual device is represented by a virtual domain (VDOM). Under each tenant, multiple virtual devices can be configured. A VDOM name is the virtual device ID that can be generated by APIC when a virtual device is added.

- From a Cisco ACI perspective, each tenant sees available interfaces and can share interfaces (ports) with other tenants if it is multicontext aware. For a physical appliance under L3 Routed (Go-To) mode, the tenant can share the physical interface as VLAN to isolate the physical interface.

Fortinet’s VDOMs provide a truly unique differentiation in the domain of multitenancy. Designed for efficient device usage and configuration management, VDOMs work extremely well with Cisco’s ACI Ecosystem.
IT administrators define service policies like high availability, virtual IP, and port forward for different applications in APIC and create service graphs to identify the set of network or service functions that are needed by the applications. When a security policy is triggered during an application deployment life cycle, Cisco APIC will force the packages to route through the Fortinet FortiADC for application delivery controls without manual configuration.
Cisco APIC integrates with Fortinet FortiADC appliances for the private cloud to simplify network security deployment. To connect the FortiADC appliance to the Cisco ACI fabric, the virtualization administrator simply needs to associate the predefined application policy with the virtual machine networks created by Cisco APIC. The Cisco ACI fabric is designed to provide overlay independence and can bridge frames to and from in the heterogeneous environments.

The physical or virtual FortiADC appliances integrate into the Cisco ACI policy and orchestration model for better application agility, automation, and lower total cost of ownership. The FortiADC XML device package can be downloaded from https://support.fortinet.com/. For more information on FortiADC product features, please visit https://www.fortinet.com/products/application-delivery-controllers/fortiadc.html. For more information on Cisco ACI, please visit http://www.cisco.com/go/aci.