CASE STUDY

ICT Provider Creates Agile Infrastructure to Securely Deliver Custom-fit Solutions to Each Hosted Client

With almost 10,000 professionals dedicated to information and communications technology (ICT), this European multinational enables its clients—spanning public, private, and government entities, as well as other service providers—to navigate the complete life cycle of ICT projects. This extends from design and deployment through to monitoring and ongoing management.

Active in 18 countries, the company offers clients the choice of selecting physical, cloud-based, and hybrid deployment options for the delivery of its broad range of IT services and hosting options. One of the fundamental tenets of its approach is to customize deliverables to precisely meet the unique needs of each customer.

Catering to individual client requirements necessitates that the company's environment is highly flexible, with the ability to adapt and scale as its own business grows and as customers' requirements evolve. A decision to build a pair of new data centers presented the opportunity to plan new facilities that incorporate a state-of-the-art approach to the delivery of services.

Designed from the Ground Up

The new infrastructure was designed to facilitate hybrid cloud integration and provide a multi-tenancy platform. A key design criterion was to incorporate the capability of supporting individual customer environments without compromising the ability to deploy products and services.

The ICT provider used ACI, a software-defined networking (SDN)-based architecture—separating the control plane and data layer of the networking stack—to simplify management and maximize resource utilization. One of the company's network specialists recalls, "Based on previous positive experiences, we leveraged a methodology based on the Cisco Application Centric Infrastructure [ACI] and supplemented it with next-generation firewalls from Fortinet to give us the necessary segmentation and security granularity."

"The integration of Cisco ACI and Fortinet can deliver accelerated software-defined security, enabling transparent security services insertion anywhere in the network. The joint solution provides enhanced visibility and security, lower TCO, and increased efficiency in service provisioning and network security segmentation."

– *Senior Manager Infrastructure, European IT Services Provider*

Details

Customer: ICT Provider

Industry: Managed Security Services

Location: Europe

Cisco ACI applies an SDN policy model across the entire network infrastructure to reduce total cost of ownership (TCO), automate IT tasks, and accelerate data-center application deployments. The company is strongly considering the use of the FortiGate Connector for Cisco ACI to tightly integrate multiple FortiGate firewalls with the Cisco Application Policy Infrastructure Controller (APIC).

The FortiGate Connector for Cisco ACI is available to all FortiGate customers—providing automated security provisioning with a full range of protection and prevention capabilities.

Tailored to Match the Needs of Each Client

The ability of ACI to deliver virtual separation enables every customer to be classified as a unique tenant, each able to access the appropriate set of services. A construct known as Endpoint Groups (EPG) facilitates variable combinations of application components to be mapped to network resources. In turn, this empowers the use of policies and rules at logical application boundaries.

Endpoint groups also deliver the granularity necessary for microsegmentation, giving great control and flexibility for defining policies such as what traffic categories have to pass through a specific FortiGate, which hosts can talk with each other, and which application modules can access external resources. EPG control is attribute-based, enabling the company to isolate or quarantine specific network components, all governed by a customizable set of predefined rules.

The microsegmentation capabilities of ACI enable users to create resilient partitions across combinations of virtual and physical domains in a consistent policy-driven framework, facilitating operational flexibility and control. ACI service graph functionality provides a logical and application-related view of services, and enables an L4/L7 device to be provisioned and shared across multiple applications and departments. Among other benefits, service graph automates management of VLAN assignments, and updates access control lists (ACLs) and Pools automatically with EP discovery and health scores collection.

The ACI fabric supports secure multi-tenancy at scale and enables complete isolation of network traffic and security policy administration for each tenant. All tenants can define their own private networks, as well as bridged domains, and security policies for their individual applications. The architecture facilitates complete separation of management, administration, and the underlying network infrastructure.

The bidirectional communication path brokered by the FortiGate Connector for Cisco ACI will further elevate the contributions of the company's FortiGate firewalls, enabling "discussions" to take place on topics such as the appearance of a previously unregistered device or the security status of a specific application module.

Another FortiGate differentiator, the virtual domain—or VDOM as it is more commonly called—facilitates a single device to act as multiple, fully featured separate entities, further enhancing the infrastructure's ability to provide microsegmented capabilities tailored to each individual customer. The network specialist describes, "We have multiple clusters of FortiGate firewalls: Fortinet's wide range of models enables us to exactly match the clients' needs, applications, and mix of services. Each customer gets set up as a tenant in ACI and is provided with a dedicated FortiGate VDOM."

Business Impact

- More compelling service offering with customized microsegmentation
- Elevated security, control, and visibility
- Investment protection through scalable, agile network infrastructure
- Operational simplicity and increased potential for automation
- Lower resource burden through centralized management

Solutions

- FortiGate
- Fabric Connector for SDN

"The Fortinet Security Fabric's integrated, collaborative, and adaptive architecture can deliver security without compromise to address our security needs. The joint solution provides enhanced visibility and security, lower TCO, and increased efficiency in service provisioning and network security segmentation."

– *Senior Manager Infrastructure, European IT Services Provider*

Adding Functionality and Visibility

The company's consultants work with customers to define the endpoint groups within their tenancy and to establish the inter- and intra-dependencies across EPGs with the use of structured contracts. Access rights can be documented within these contracts using ACLs. Security and forwarding policies also can be dynamically assigned to these groups.

In its default configuration, the Cisco ACI can only utilize stateless ACLs, limiting analysis to packet headers. The FortiGate firewalls can be added to provide stateful inspection—enabling an in-depth examination of multiple packet parameters, including source, destination, and payload. "The ability of a FortiGate to perform a stateful assessment gives us additional functionality and enhanced visibility," comments the network specialist.

He adds, "A lot of internal traffic doesn't need to pass through a firewall, so the FortiGate firewall's ability to perform stateful inspections enables us to determine—on a packet-by-packet basis—the necessary handling and degree of scrutiny to apply. Being able to achieve this level of granularity is a compelling feature of our infrastructure."

The company's staging environment leverages a FortiGate firewall integrated into the network infrastructure using the FortiGate Connector for Cisco ACI. Server-to-server traffic ("east-west") is assigned a FortiGate VDOM that handles tasks such as provisioning, new rules, interface definitions, and device packages. Similarly, a second VDOM is dedicated to client-server ("north-south") communications.

With the exponential rise in cyber-threat volumes and sophistication, security has become a critical concern around the globe. Conventional perimeter defenses are no longer capable of protecting IT infrastructures. For the team, the Fortinet-Cisco partnership—with the potential addition of the FortiGate Connector for Cisco ACI—is providing a foundational layer with the agility and security necessary to meet the challenge.

"The integration of Cisco ACI and Fortinet can deliver accelerated software-defined security, enabling transparent security services insertion anywhere in the network through single-pane-of-glass management," says the company's senior manager for infrastructure. "The Fortinet Security Fabric's integrated, collaborative, and adaptive architecture can deliver security without compromise to address our security needs. The joint solution provides enhanced visibility and security, lower TCO, and increased efficiency in service provisioning and network security segmentation."

December 10, 2019 11:02 PM

540065-0-0-EN

D:\Fortinet\Case Study\Anon European\cs-FA-anon-european\cs-FA-anon-european