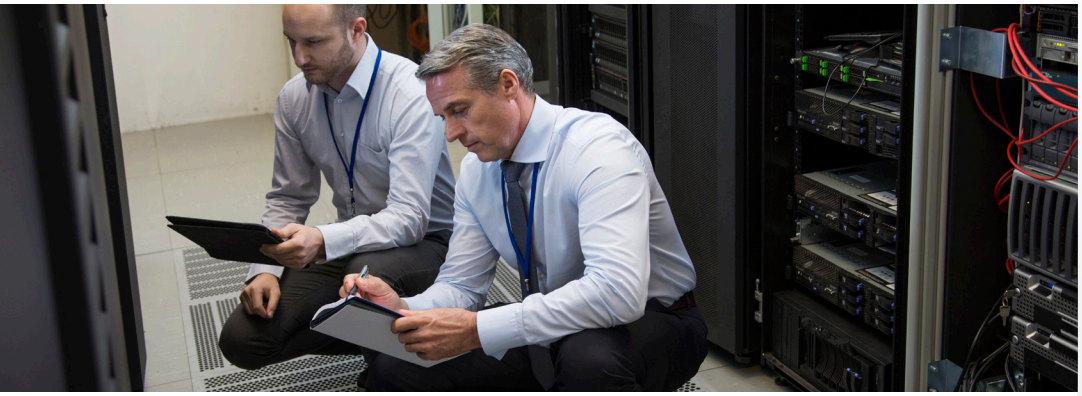
ICT PROVIDER CREATES AGILE INFRASTRUCTURE TO SECURELY DELIVER CUSTOM-FIT SOLUTIONS TO EACH HOSTED CLIENT



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 lifecycle of ICT projects; 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 datacenters 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, recalled, "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."

Cisco Application Centric Infrastructure applies an SDN policy model across the entire network infrastructure to reduce total cost of ownership, 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.

"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: Anonymous

INDUSTRY: IT Services

LOCATION: Europe

ANTICIPATED BUSINESS IMPACT

- Clients attracted by ability to microsegment environment to meet their own requirements
- Best-in-class pairing delivers elevated security, control and visibility
- Scalable, agile network infrastructure provides investment protection
- Operational simplicity and increased potential for automation
- Centralized management lowers resource burden

SOLUTIONS

- FortiGate
- Cisco ACI
- FortiGate Connector for Cisco ACI

TAILORED TO MATCH THE EXACT 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 empowering the use of policies and rules at logical application boundaries.

Endpoint groups also deliver the granularity necessary for micro-segmentation; 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, which application modules can access external resources, etc. 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 micro-segmentation 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 ACLs and Pools automatically with EP discovery and health scores collection.

The ACI fabric supports secure multitenancy 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 bi-directional communication path brokered by the FortiGate Connector for Cisco ACI will further elevates the contributions of the company's FortiGates, 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 micro-segmented capabilities tailored to each individual customer. The network specialist described, "We have multiple clusters of FortiGates: Fortinet's wide range of models enables us to exactly match the clients' needs, applications and mix of services. Each customer gets setup as a tenant in ACI and provided with a dedicated FortiGate VDOM."

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 access control lists (ACLs). Security and forwarding policies also can be dynamically assigned to these groups.

In its default configuration, the Cisco Application Centric Infrastructure 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," commented the network specialist.

He added, "A lot of internal traffic doesn't need to pass through a firewall, so the FortiGate'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 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 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," stated 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."

software-defined security, enabling transparent security services insertion anywhere in the network through single-pane-of-glass management," stated Erik Sohlman, senior manager infrastructure at Axians. "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."

GLOBAL HEADQUARTERS
Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
United States
Tel: +1.408.235.7700
www.fortinet.com/sales

EMEA SALES OFFICE
905 rue Albert Einstein
06560 Valbonne
France
Tel: +33.4.8987.0500

APAC SALES OFFICE
300 Beach Road 20-01
The Concourse
Singapore 199555
Tel: +65.6513.3730

LATIN AMERICA HEADQUARTERS
Sawgrass Lakes Center
13450 W. Sunrise Blvd., Suite 430
Sunrise, FL 33323
Tel: +1.954.368.9990

99209-A-0-EN Aug 7, 2017 8:37 AM
Macintosh HD:Users:mbunnell:Desktop:CS-Anon-European-IT:cs-anon-european-it.indd