FORTINET | Alibaba Cloud

SOLUTION BRIEF

Fortinet Extends Advanced Security for Alibaba Cloud

Executive Summary

Fortinet and Alibaba are working together to bring best-in-class cybersecurity to organizations using Alibaba Cloud for digital transformation (DX) and global e-commerce. The Fortinet Security Fabric provides broad coverage across the attack surface—from the Internet of Things (IoT) to the cloud—while integrating each of the security elements and automating threat protection. The Security Fabric offers organizations advanced, extensible threat protection that spans clouds and data centers and provides comprehensive security tools supported by the industry's leading threat research team backed by a global network of sensors and machine-learning (ML) technology. It also delivers centralized management and analytics, automation, and intent-based segmentation that enables organizations to reduce risk, even in dynamically changing networks.

Securing Digital Transformation in the Alibaba Cloud: Use Cases

The Fortinet Security Fabric protects business workloads across on-premises data center and cloud environments, including multilayered security for born-in-the-cloud applications. The Security Fabric supports a variety of common Alibaba Cloud-based use cases.

Protecting Cloud Workloads

Applications being built in or migrated to the cloud need to be protected against traditional internet-borne threats, as well as from new threats that are introduced via application programming interfaces (APIs) that propagate across workloads.

The combination of inline protection for north-south traffic, host-based protection for east-west traffic, and protection for cloud API and configuration risks offers the tightest security solution for the cloud. **FortiGate VM** protects virtual cloud networks from internet-based threats and provides secure multi-cloud connectivity. **FortiClient** endpoint protection on virtual machines (VMs) extends security within the cloud to ensure security policy compliance. **FortiCASB Cloud** protects from unwanted or unsupervised configurations at the cloud-account level.

Securing Hybrid Clouds

Secure connectivity between cloud environments and data centers is requisite for cloud computing projects. Often the need for secure communications leads to limited insight into the threats that may travel with network traffic. Meanwhile, complex, multi-cloud deployments expand the attack surface and create challenges in terms of establishing and enforcing consistent security policies. Securing hybrid clouds requires a security fabric that will work across data centers and clouds to provide single-pane-of-glass management and analytics.

Alibaba Cloud

Alibaba Cloud provides comprehensive global cloud computing services that power e-commerce and digital transformation worldwide. Alibaba Cloud offers high-performance, elastic computing power in the cloud. Services are available on a pay-as-you-go basis and include data storage, relational databases, big-data processing, distributed denial-of-service (DDoS) protection, and content delivery networks (CDN). Alibaba Cloud operates 58 availability zones in 20 regions around the world.

83% of enterprise workloads will be in the cloud by 2020, with 63% of IT professionals listing security as their biggest concern about this trend.[1]

Over 80% of enterprises have adopted two or more public clouds, with nearly two-thirds using three or more.[2]

FortiGate next-generation firewalls (NGFWs) and cloud security solutions offer best-of-breed secure connectivity, network segmentation, and application security for hybrid-cloud deployments. These solutions connect through a high-speed VPN tunnel to provide centralized, consistent security policy enforcement. **FortiGate VMs** deployed in the public cloud can securely communicate and share consistent policies with FortiGate NGFWs of any form factor—whether provisioned across clouds or in a private data center.

Using Intent-based Segmentation

Relying on static trust zones for users, devices, and applications is no longer sufficient when it comes to threat protection. In particular, for cloud deployments, network segmentation based on static IP addresses is unable to keep up with the dynamic nature of today's networks. To address this issue, FortiGate VMs provide **intent-based segmentation**, which builds access rules and network segments based on business logic. Intent-based segmentation then adjusts rules dynamically in response to a continuous trust assessment of users, devices, and applications. For intent-based segmentation in the cloud, FortiGate VMs leverage metadata or tags associated with resources across multiple clouds to enforce security policies based on business-access needs.

Nearly one-third of organizations say it is difficult to get a holistic perspective on external threats due to disaggregation of threat intelligence.[3]

Cloud-based Security Management and Analytics

Fortinet leverages the multiregional and global presence of top cloud infrastructure providers to deploy centralized and global security management and analytics systems in the cloud. **FortiManager VM**, **FortiAnalyzer VM**, and **FortiSIEM VM** can all be deployed in the cloud and all can scale to monitor and secure vast, multi-cloud deployments. FortiManager integrates visibility and control of FortiGate NGFWs across on-premises and cloud environments into a single pane of glass, while FortiAnalyzer aggregates and reconciles threat intelligence across the Fortinet Security Fabric. The latter is assessed based on government and industry regulations as well as security standards, enabling organizations to identify vulnerabilities in real time and proactively detect, prevent, and respond to threats.

How the Security Fabric Complements Alibaba Cloud Security

The Fortinet Security Fabric provides Alibaba Cloud users with the ability to apply universal policies throughout their multi-cloud infrastructures for consistent policy enforcement and global visibility. The Security Fabric offers deep, multilayer protection and operational benefits for securing web applications over Alibaba Cloud and for managing global security infrastructures from the cloud.

The value proposition of Alibaba Cloud plus Fortinet Security Fabric includes:

- **Single-pane-of-glass control and management.** Both cloud and on-premises resources can be managed from Alibaba Cloud. This simplicity helps eliminate human errors while reducing the time burden on limited IT resources.
- **High availability (HA).** FortiGate VM ensures that security services in Alibaba Cloud are available 24×7. Fortinet employs a pair of FortiGate VM NGFWs utilizing FortiGate Clustering Protocol (FGCP) in unicast form to provide an active-passive clustering solution for deployments in Alibaba Cloud. This provides fast and stateful failover of security services without the need for external automation or services. The FortiOS operating system provides session and configuration synchronization of firewall, IPsec/SSL VPN, and Voice-over-IP (VoIP) sessions.
- **Cloud-native visibility and control.** Organizations gain in-depth visibility into their Alibaba Cloud application deployments. They no longer need to care for specific deployment configuration details, but rather get closer to an intent-based segmentation. Dynamic address groups and logical naming of cloud-based resources allow security policies to be followed when underlying resources scale-out or move throughout the cloud infrastructure.

- **Shadow IT control.** With organizations streamlining IT operations and consolidating security controls, many lines of business now directly source their own cloud-based services. The Security Fabric offers IT departments better visibility into the use of Alibaba Cloud infrastructures and the ability to implement tighter control over usage patterns to protect the organization from risk.
- **PCI compliance ready.** Fortinet solutions offer best-in-class protection to help ensure compliance with the current version of the Payment Card Industry Data Security Standard (PCI DSS).

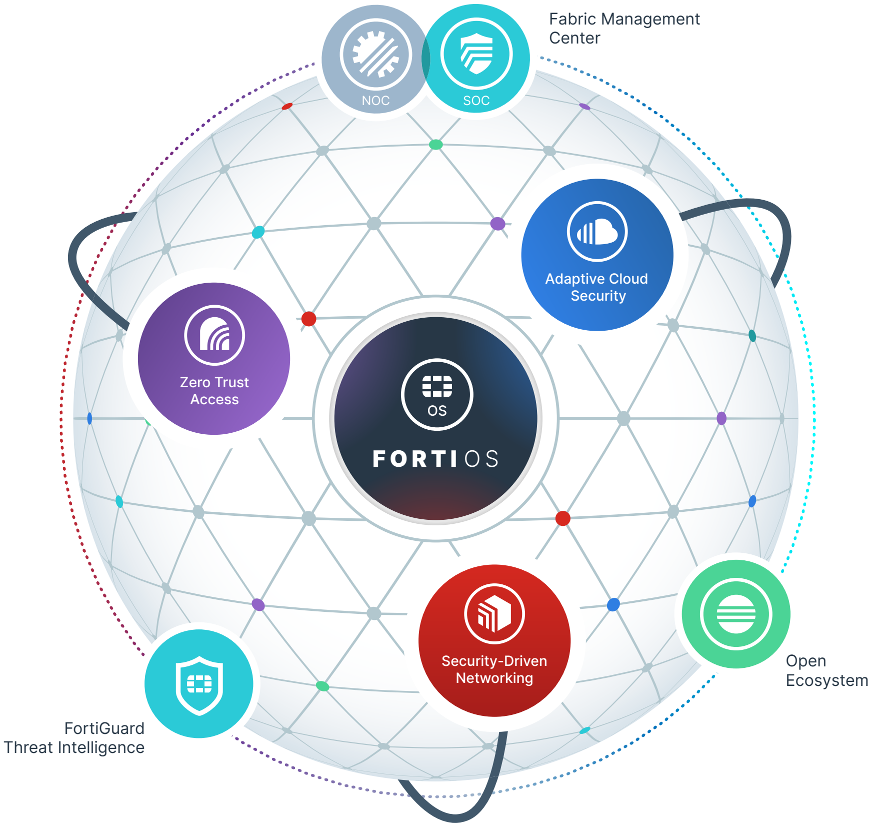

Figure 1: Fortinet Security Fabric diagram.

Integrated Defenses That Span the Full Attack Spectrum

The Fortinet Security Fabric secures traffic, data, and applications while increasing confidence in Alibaba Cloud environments. All Fortinet cloud products are based on Fortinet VM form factors. And licenses purchased from a Fortinet channel partner for VMs are transferrable across platforms. For example, using a **bring-your-own-license (BYOL)** model, the same VM license for FortiGate VM on VMware will work for FortiGate on the Alibaba Cloud platform. In addition, FortiGate, FortiAnalyzer, and FortiManager are all available in the Alibaba Marketplace.

The Fortinet Security Fabric for Alibaba Cloud includes the following Fortinet solutions:

- **FortiGate VM** NGFWs deliver industry-leading threat protection to defend against known, unknown, and zero-day cyberattacks. FortiGate VM automatically scales to provide the necessary visibility and protection as fluctuating workload demands expand and contract. This auto-scaling capability ensures security while minimizing costs during slow or idle periods.
- **FortiWeb** web application firewalls (WAFs) protect hosted web applications against attacks from advanced exploits. Using multilayered and correlated detection methods, FortiWeb defends applications from both known and unknown vulnerabilities and zero-day threats. When combined with the Fortinet Web Application Security Service, organizations are protected from the latest application vulnerabilities, bots, and suspicious URLs. With dual ML detection engines, applications are safe from sophisticated threats such as SQL injection, cross-site scripting, buffer overflows, cookie poisoning, malicious sources, and DDoS attacks. FortiWeb is also available as a BYOL VM.

- **FortiManager** provides single-pane-of-glass management across the extended enterprise. It enables both central policy management and insight into networkwide traffic and threats. It includes features to contain advanced threats as well as industry-leading scalability to manage up to 10,000 Fortinet devices.
- **FortiAnalyzer** collects, analyzes, and correlates data from Fortinet products for increased visibility and robust security alert information. When combined with the FortiGuard Indicators of Compromise (IOC) Service, it also provides a prioritized list of compromised hosts to enable rapid response actions.
- **Fabric Connectors** enable open integration of the Fortinet Security Fabric to automate firewall and network security insertion into dynamic network flows with multiple components in a customer's ecosystem.

Multilayered, Shared Responsibility Protection That Reduces Risk

Protecting organizations from the onslaught of advanced, constantly evolving threats is a difficult undertaking. The combination of Alibaba Cloud and the Fortinet Security Fabric provides organizations with the ability to extend security visibility and control from the data center to the cloud, from users and devices to the wireless access point.

Multilayered security, intent-based segmentation, and ML-enabled security capabilities, which are a key foundation of the Security Fabric, form a comprehensive shared responsibility model that streamlines operations and policy management for improved security life-cycle management. Plus, the combination of Alibaba Cloud and the Fortinet Security Fabric gives organizations a scalable security platform with low total cost of ownership.

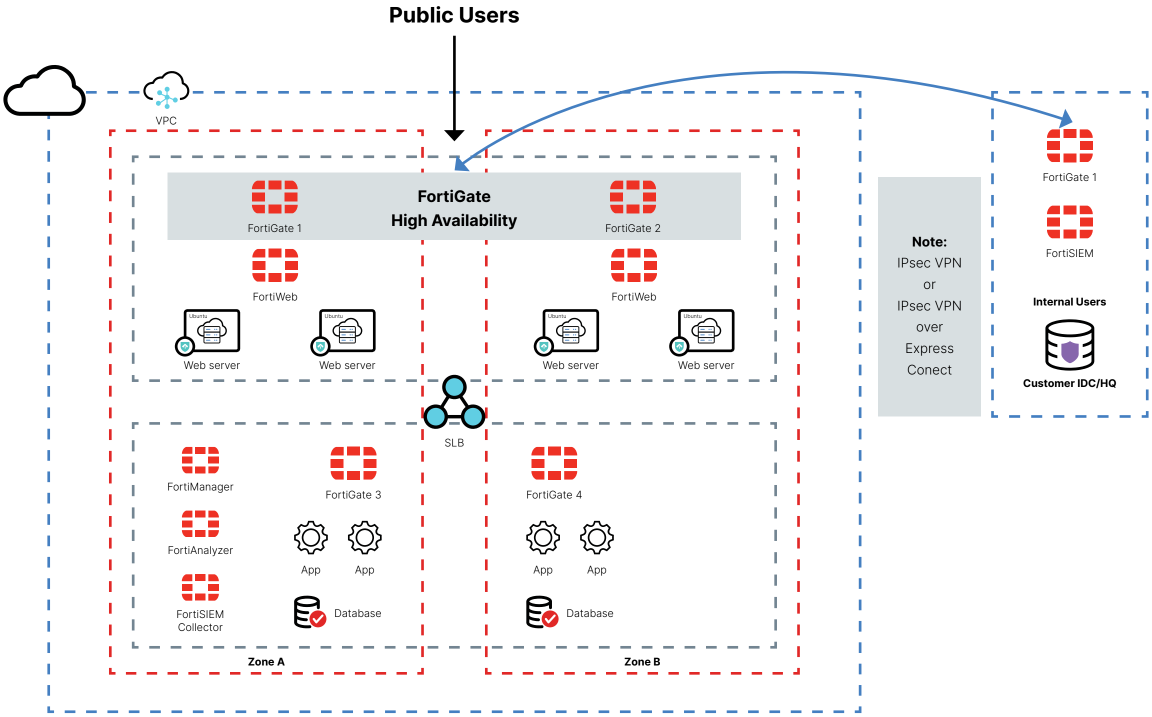

Figure 2: Alibaba reference cloud security architecture.

[1] Louis Columbus, "83% Of Enterprise Workloads Will Be In The Cloud By 2020," Forbes, January 7, 2018.

[2] Mike Kelly, "Multicloud: the new monitoring silo," InfoWorld, June 22, 2018.

[3] Jon Oltsik, "Operationalizing threat intelligence," CSO, July 5, 2016.

www.fortinet.com

March 30, 2021 5:32 AM

D:\Fortinet\2021 Rebranded templates\Marketing or Comms Request\March\Branding Refresh\913517 - Update Connecting SBs\sb-FA-fortinet-and-alibaba-cloud-3302021\sb-FA-fortinet-and-alibaba-cloud-3302021

448192-A-0-EN