SOLUTION BRIEF

Consistent Hybrid and Multi-Cloud Network Security to Power Digital Acceleration

Executive Summary

Digital acceleration (DA) is powering organizations of various sizes and in diverse sectors to deliver higher productivity, increase the speed of business, and improve their cost structures. Moreover, as part of DA, applications can now live anywhere that best meets DA outcomes from the physical and virtual data center to multi-cloud to edge compute. This introduces many network security challenges across the expanded attack surface. Protecting applications where they live with consistent security and centralized visibility and management is critical to the success of DA initiatives.

Over 76% of organizations have a hybrid cloud or multi-cloud deployment.[1]

FortiGate VM Delivers Comprehensive Cloud Network Security

IT infrastructure and business applications running in cloud, physical and virtual data centers, and virtual branch deployments are constantly under attack by external and internal threats. Without effective threat protection, organizations could face financial impact and loss of reputation. They face challenges with fragmented solutions and point products creating security gaps and increasing risks.

The network firewall continues to be the most effective tool for securing business applications and data both on-premises and in the cloud. It reduces deployment complexity, development costs, and demands on skillset to efficiently deliver an effective security posture.

Fortinet FortiGate high-performance appliances protect applications running in the data center. Organizations running FortiGate appliances benefit from converged networking and security capabilities in a single solution that is backed by the Fortinet Security Fabric and FortiGuard Security Services and threat intelligence.

Fortinet FortiGate VM virtual next-generation firewall runs the same FortiOS secure networking operating system as the physical FortiGate firewalls, delivering enterprise-grade security at any scale across the entire attack surface to effectively protect public and private clouds, virtualized data centers, and virtualized branches. As a result, organizations get consistent security policies across everywhere FortiGates are deployed regardless of form factor; with this, they also get centralized visibility and management.

Advanced capabilities

Converged security and networking

FortiGate VM protects networks and applications with high-performance next-generation firewall security, offering advanced routing features to deploy secure networks at any scale, and supporting SD-WAN to intelligently steer application traffic and improve end-user experience. It delivers these advanced features in one virtual form factor.

Advanced protection

The threat landscape is continuously evolving and attacks are increasingly becoming more and more sophisticated. To counter these threat vectors, FortiGate VM utilizes artificial intelligence (AI) and machine learning (ML) powered by FortiGuard Global Threat Intelligence for stopping advanced attacks.

Automation

To enable agility for operations teams, FortiGate VM supports automation with cloud-specific template tools and cloud-agnostic third-party frameworks. IT teams can deploy network security in minutes, easily scale operations, and integrate into DevOps workflows.

Key Use Cases

Security in virtualized data centers and private clouds

The majority of the organizations are transforming their traditional data centers into virtualized data centers or private clouds, where they use software-defined networking (SDN), remote worker and virtual desktop infrastructure (VDI). These technologies bring in new security challenges.

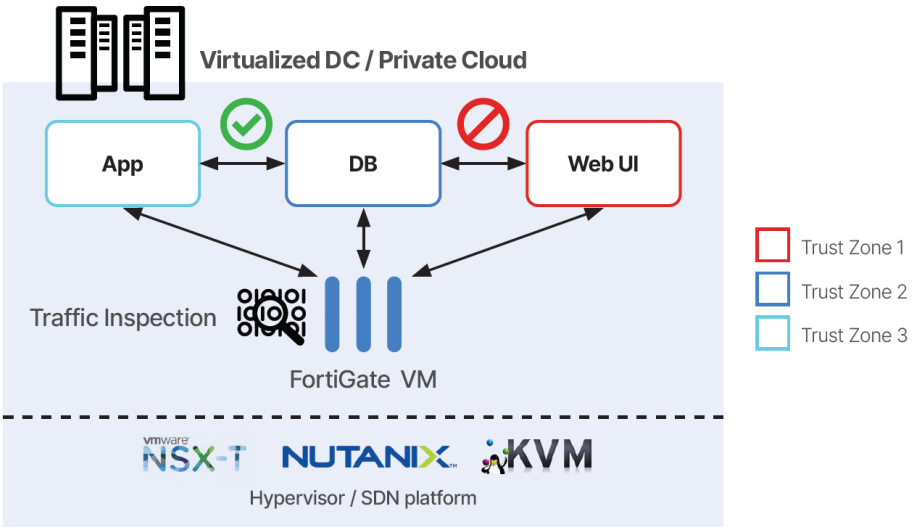


Figure 1: East-west protection of workloads

SDN environments like VMware NSX and Nutanix Flow are not only used for virtual networks but are sometimes used for microsegmentation of the virtual workloads. This approach is marginal; threats can be hidden deep in traffic flows allowed between trust zones, and it can lead to lateral propagation of attacks. FortiGate VM supports service chain integration with these SDN platforms and to allow agile insertion of advanced security services, such as IPS, AMP, sandboxing, AV, or DNS security, between microsegments to inspect and protect allowed traffic and protect the east-west perimeter.

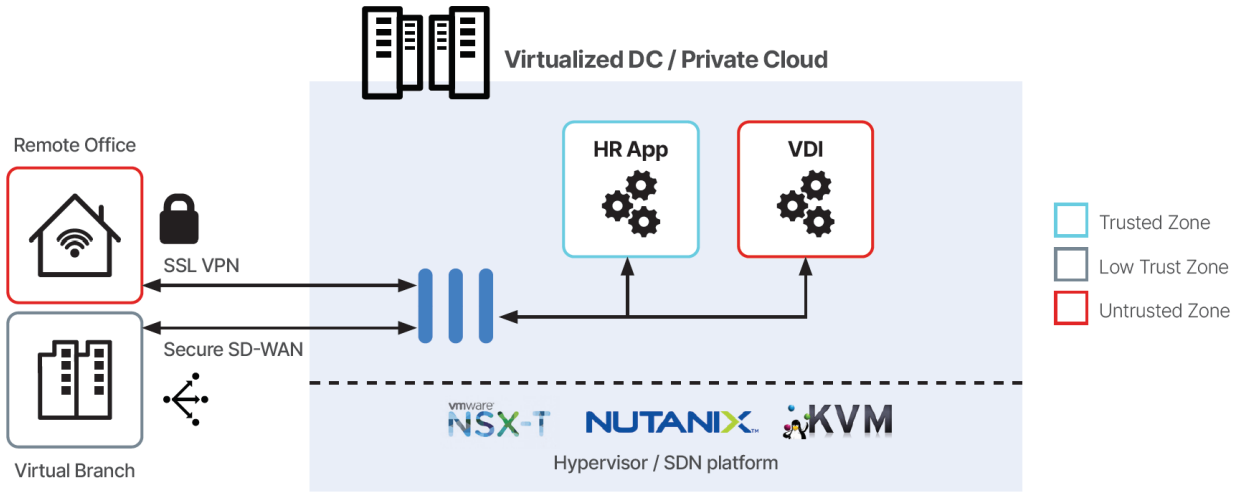
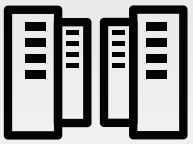


Figure 2: Secure access and segmentation

Today, organizations seek to provide secure user access to IT applications from any location. With VDI and remote working adoption, network traffic can come from uncontrolled or user-controlled devices into the core of the IT data center, creating opportunities for threat actors to exploit vulnerabilities and attack other sensitive workloads. FortiGate VM can be used to segment traffic to and from these locations into trust zones to prevent the spreading of threats. Also, the network traffic from these locations may traverse the internet and other unsecured networks. FortiGate VM supports SSL-VPN to securely connect remote workers and secure SD-WAN connectivity to securely connect virtual branch locations, which improves both security and application performance.

In deployments with many FortiGates, FortiManager can be used to unify virtual and physical firewall policy infrastructure to simplify deployment and operation of network security.



Lack of visibility (49%), not enough control (42%), and lack of staff resources or expertise (40%) remain to be top challenges for organizations.[2]

Secure connectivity into the cloud

Many organizations are lifting specific applications needing global access or elastic scaling and shifting them to the public cloud. They need to, however, provide a secure connectivity path to access these cloud application workloads. Cloud providers offer VPN gateways to get the user traffic into their virtual private clouds (VPC or VNet) but there several limitations to this approach. Typically, organizations use a different on-premises VPN appliance, and the addition of a cloud provider gateway increases management complexity. Moreover, for SSL VPN, the cloud provider offers a totally different service. The cloud IPSec VPN gateway is also limited in bandwidth, which makes it a non-starter for many large enterprises.

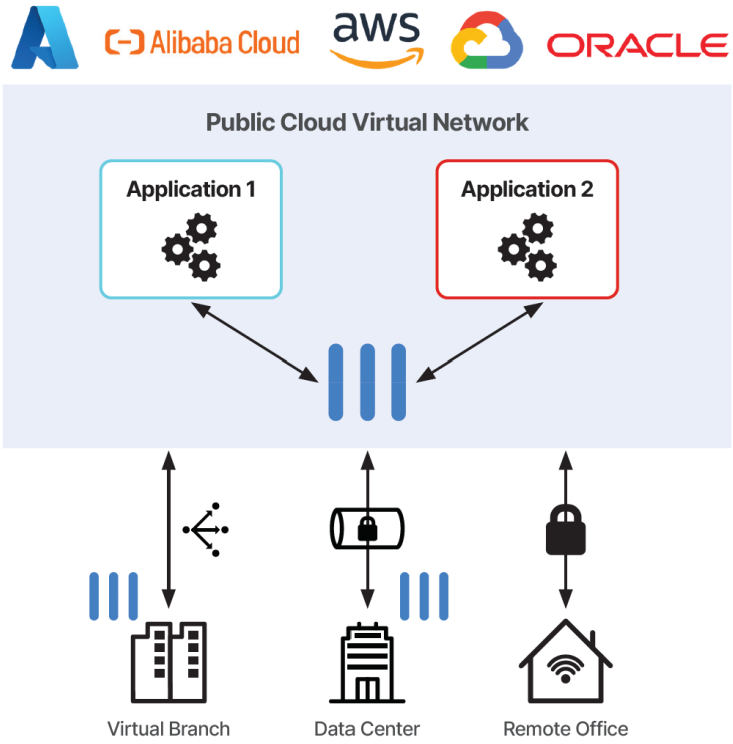


Figure 3: Secure connectivity into public cloud

FortiGate VM can be used to reduce complexity in connecting to the public cloud by utilizing it both at the virtual branch and in the VPC or VNet. Not only that, but it can also be used for SSL VPN connectivity from remote users, IPSec VPN connectivity from the data center, and SD-WAN connectivity from branch locations. FortiGate VM comes in various sizes to scale-up IPsec bandwidth and can be used with a cloud provider load balancer to scale-out SSL VPN access capacity. By offering key connectivity options with high performance, FortiGate VM secures connectivity into the public cloud.

Security in the public cloud

In the expansion phase of their cloud transformation organizations spin-up multiple virtual networks (VPCs) with some reaching hundreds of VPCs. They face both network routing and security issues. The higher count of VPCs and cloud workloads also means increased risk and more vulnerabilities and the lack of any access control between workloads and VPCs can result in lateral attacks and data exfiltration.

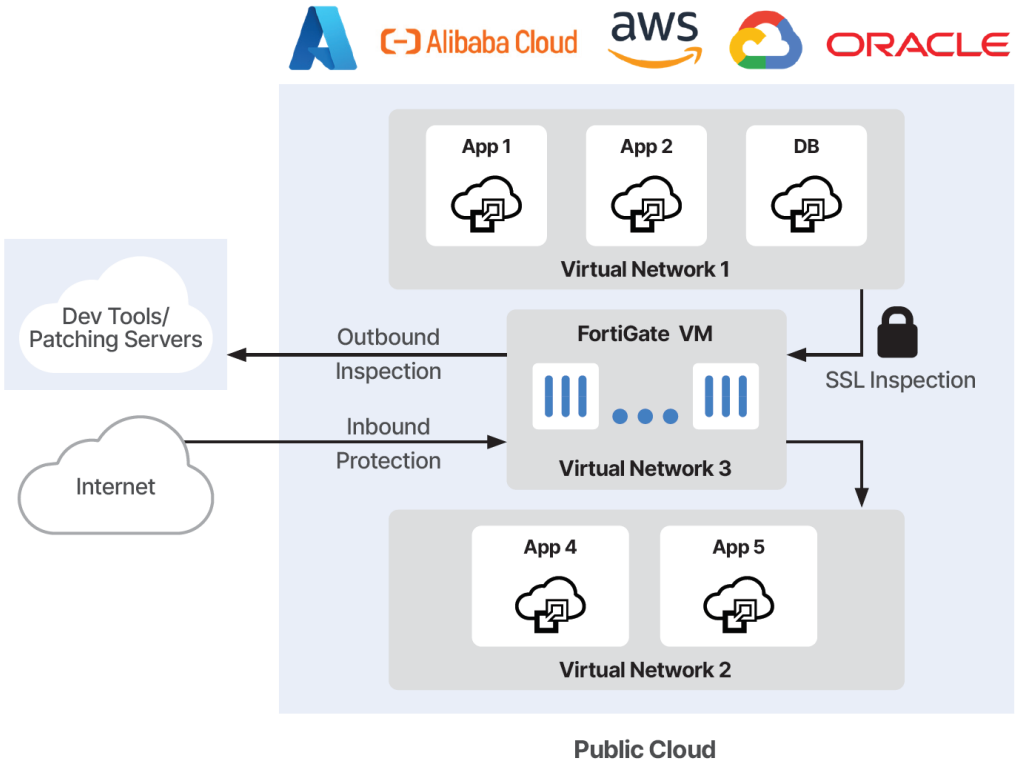


Figure 4: Secure perimeter in public cloud

FortiGate VM can be used for getting deep visibility into application workload traffic to ensure IT and regulatory compliance. In many cases, application workloads access developer tools like GitHub and patching servers to get OS and application updates. FortiGate VM can employ URL filtering to inspect and control this outbound traffic. These cloud applications are accessed by various user types from many locations, FortiGate VM supports advanced security capabilities like IPS, sandboxing, anti-malware protection (AMP), and antivirus (AV) to provide protection against external malicious attacks launched over the internet. Organizations with larger cloud deployments may want to centralize security inspection and routing across VPCs to simplify security operations and apply compliance policies more effectively. With support for BGP routing and advanced threat protection, FortiGate VMs can be deployed in high-availability mode in a centralized VPC called Security Services Hub to simplify networking and deliver enterprise-grade security in the public cloud.

Security across multiple clouds

The move to multi-cloud comes with technical challenges, specifically routing and security of application traffic to each cloud, within each cloud, and across clouds. Organizations also need to provide high-speed connections from on-premises locations like branches, data centers, and remote workers to deliver the best possible application experience. At the same time, however, organizations need to reduce operational overhead and management complexity by utilizing products and services that remove the need for multiple disjointed cloud-provider consoles. Another important challenge posed by these multi-cloud deployments is fragmentation of network and security policies across cloud deployments and on-premises locations.

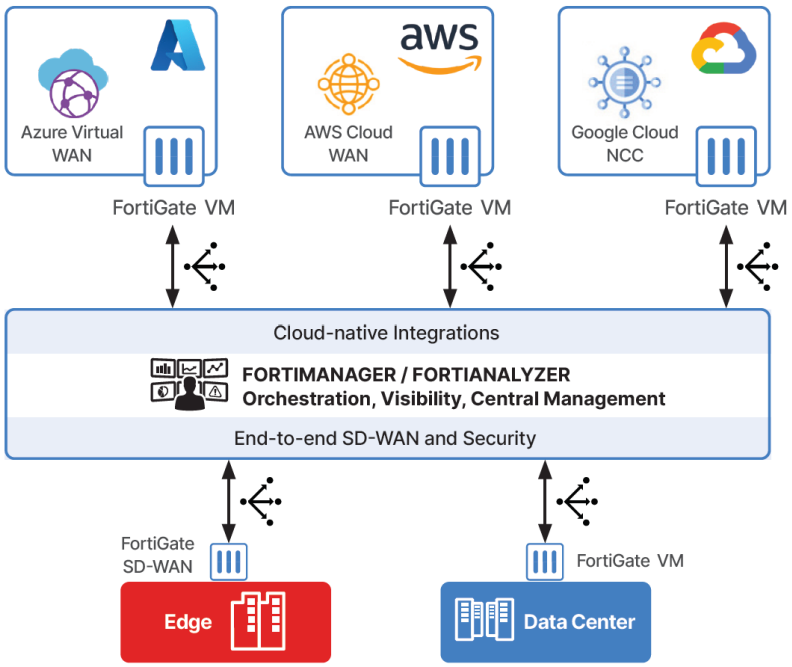


Figure 5: Secure multi-cloud SD-WAN

FortiGate VM provides SD-WAN connectivity and continuous visibility into threats across multiple clouds and virtual data centers. Secure multi-cloud SD-WAN capability supported on FortiGate VM is tightly integrated with cloud-native managed network services like Azure Virtual WAN, AWS Cloud WAN, and Google Network Connectivity Center, and this enables IT teams to simplify traffic routing to and from on-premises locations into the respective cloud VPCs and VNets. The SD-WAN overlay network can be used to connect application workloads across clouds with consistent network policies and deliver better application experience. FortiGate VM can also be deployed as part of a fabric of firewalls on multiple clouds to enforce consistent security policies and establish an effective security posture.

Single-pane-of-glass management and analytics

The proliferation of management consoles for different point products imposes a huge burden on management and operations. Organizations are increasingly seeking a unified management solution that will enable them to establish uniform security policies, maintain consistency between on-premises security and cloud security, and achieve continuous visibility across clouds.

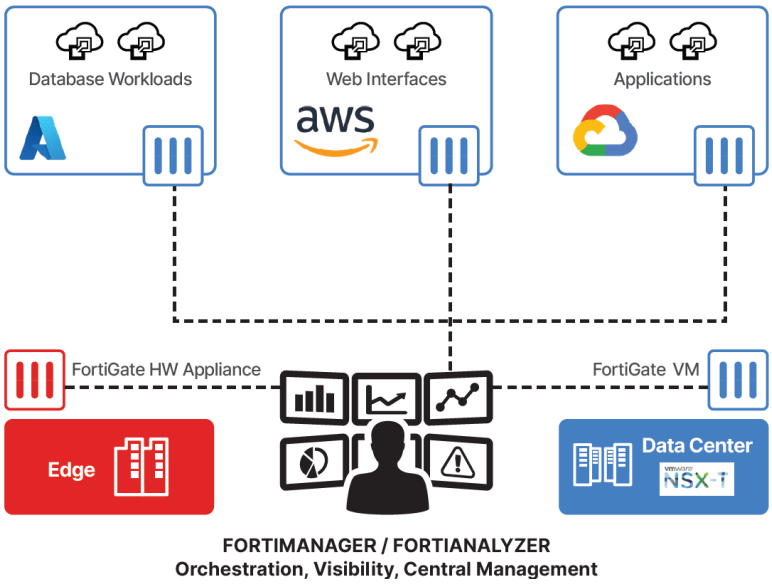


Figure 6: Single-pane-of-glass management

FortiManager provides single-pane-of-glass management for defining security policies on FortiGate VMs and physical FortiGates, which simplifies security management across cloud, virtual/physical data center, and branch locations. It also supports fabric connectors that utilize APIs to integrate with cloud providers and SDN platform-management tools. With these integrations, it can be used to orchestrate security policy in a multi-cloud deployment. FortiAnalyzer provides network operations center teams with valuable network analytics and insight. It can be used to get continuous visibility from FortiGate VMs and physical FortiGates across multiple deployments, including cloud and on-premises locations. Organizations can therefore simplify the management and operations of cloud networks.

Summary

With FortiGate and FortiGate VM solutions, organizations can enable hybrid and multi-cloud applications without complexity. They can innovate faster in both public cloud and virtual data center environments without increasing risks or impacting compliance, and IT teams can deliver better application experiences to remote workers, partners, and customers. Additionally, organizations benefit from reduced complexity and operational overhead with consistent security across everywhere their applications live.

Key Benefits of FortiGate VM:

- Reduce deployment and operational complexity with consistent protection and centralized management for different environments
- Leverage cloud and SDN investments through FortiGate VM integrations with cloud provider services and SDN platforms
- Improve application experience for end-users by delivering higher bandwidth through scale-out or scale-up architectures
- Tap into cloud-like on-demand consumption with dynamic changes even for virtualized data center and virtual branch deployments

[1] 2022 Cloud Security Report, Cybersecurity Insiders.

[2] Ibid.

www.fortinet.com

Copyright © 2023 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

February 17, 2023 10:26 AM
1974766-0-0-EN