FortiGate Deployment Use Cases on Microsoft Azure

Referencing the cloud is typically about infrastructure as a service (IaaS), where the customer places their trust in the cloud provider for managing and maintaining hardware. With Microsoft owning the operating system, server components, runtime, database, and identity access management (IAM), etc., to a certain extent it also represents a great portion of the platform as a service (PaaS). Also, the products like Azure website, Azure Active Directory Service, Microsoft Office 365, and workspace products are software as a service (SaaS). Security is still an important consideration with SaaS, as an insecure configuration can be just as much of a risk as an insecure virtual machine. For example, a misconfiguration of Azure Active Directory could result in an unauthorized user gaining access to something they shouldn't. For customers, to understand their role in the cloud is the first step to help translate the shared responsibility. The diagram below demonstrates how management responsibilities are shifted from the customer to the cloud.

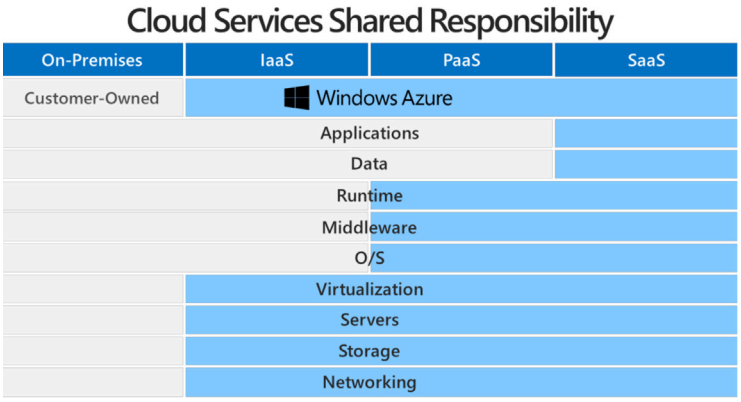


Figure 1: Separation of Roles and Responsibilities in a Cloud Environment

Full Stack of Threats in the Cloud

Traditional threats will continue to exist in the cloud, such as cross-site scripting (XSS) or SQL code injection attacks, denial-of-service (DOS) attacks, or credential-guessing attacks. Some old threats are mitigated, since patching may be automated (for PaaS only), and cloud resiliency improves failover across a service.

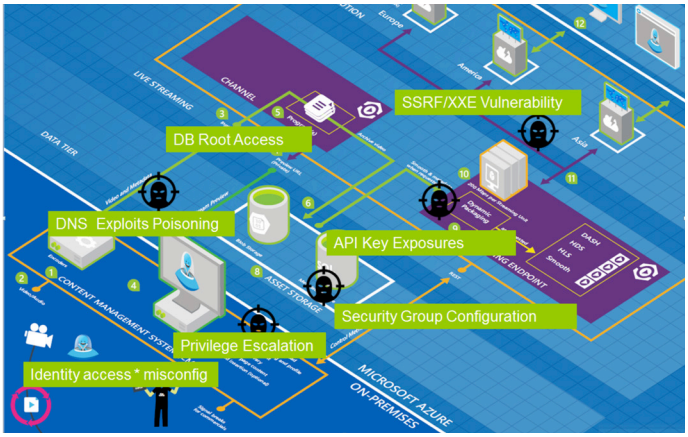


Figure 2: Full Stack of Cloud Attacks in Hybrid Cloud

The threat landscape changed when the cloud was introduced. The cloud is essentially a set of APIs used to orchestrate abstracted platform components. Some threats evolved and expanded. For example, data privacy and privileged access experienced new threats and new privilege escalation attacks (VM to host or VM to VM), jail-breaking the VM boundary or hyper-jacking (a rootkit attack on the host or VM). Fortinet has taken extraordinary measures to protect Microsoft Azure against these new classes of threats.

Terminology

Before we start, it's good to have a quick understanding about Fortinet products available on Azure. These Azure Virtual Machines run on virtual hard disks (VHDs) stored in Windows Azure Blob Storage.

FortiGate Multi-threat Security

Enterprise firewall with comprehensive threat protection, VPN (IPsec and SSL), intrusion prevention (IPS), and antivirus technologies

FortiWeb Web Application Firewall

Protect, balance, and accelerate web apps for improved security and PCI compliance

FortiManager Centralized Management

Command and control for Fortinet infrastructure in a single console

FortiAnalyzer Centralized Reporting

Aggregates log data for forensic analysis, vulnerability assessments, and compliance

FortiMail Mail Security Gateway

All-in-one inbound and outbound protection for email security gateway

These products are available with a perpetual bring-your-own-license model in the Fortinet product listing in the Azure Marketplace. There is also an additional Azure Resource Manager (ARM) template that is purpose-built for instant high-availability (HA) configuration for security protection.

ARM Template Deployment

In addition to Marketplace BYOL deployment, Fortinet provides a GitHub repository that hosts ARM templates that you can download and customize the configuration for your needs. ARM templates are JSON files that describe the resources required for individual resources such as network interfaces, a complete virtual appliance, or even an entire application stack with multiple virtual machines. The highly desired HA ARM template is a preconfigured active-passive template that helps streamline the deployment process. You can customize the template file for your Azure VNet deployment.

Azure Cloud Access Models

There are two key Azure capabilities related to cloud security:

- User-Defined Routes (UDR) that *enable configuration of routes within Azure*
  - » Control traffic flow
  - » Attach routes to subnets
  - » Specify next hop for any address prefix
  - » Set default route to force tunnel to on-premise or appliance
- Virtual Networks (VNets) that *represent the user's network in the cloud*
  - » Interconnected VNets using private IPs
  - » Can be in different subscriptions
  - » Control network settings: DHCP | DNS | Policy | Routing | Subnets

Securing Windows Azure IaaS Virtual Machines

In order to protect assets (virtual servers) within the VNet, a typical FortiGate enterprise firewall deployment requires all external communication to route through it. This makes it impossible to use public IP addresses, which are directly assigned to other virtual machines. It is possible to reassign the public IPs to a load balancer in front of the FortiGate and forward that traffic through the FortiGate, but if you were to enable direct communication with the VM, your servers would no longer be protected by the FortiGate appliance.

Communication Over VPN Tunnels

In order to allow communication over the VPN tunnels, the Azure subnets need to have a route (via a UDR) assigned to each subnet, which has the next hop for those networks as the internal interface of the FortiGate appliance.

In order to reach a VM behind a firewall in Azure, you will need to route the traffic through the firewall. Depending on how you deploy it, this will be done with the public IP of the FortiGate or a public IP assigned to the Azure Load Balancer.

If the public IP address is assigned to the Azure Load Balancer, you must configure NAT rules in the Azure Load Balancer config (in the case of a single FortiGate VM) or load balancing rules (for HA deployments) to forward the port (for example, 3389 for remote desktop) to the FortiGate.

If the public IP address is assigned to interface Nic0/Port1 of the FortiGate, all layer 4 ports will automatically be NATed directly to the private IP address assigned to the same port, thus traffic destined to 3389 will be directed to the FortiGate appliance.

In both of the above cases, you must then configure the FortiGate to translate that traffic and allow it to be accessed by the internal host. To do so, you would create a new virtual IP in FortiGate instance.

- Under “Policy & Objects” -> “Objects”
- Assign the virtual IP a name (this will be used later when creating the policy)
- For “External IP Address,” put the IP that is assigned to the interface Port1 (you will put this twice, as the range will be only that single IP)
- For “Mapped IP Address,” put the rfc1918 IP (not the public IP) that is assigned to your internal VM (again use this IP twice for a range of 1)
- Check the box next to “Port Forwarding” and select “TCP.” For “External Service Port” and “Map to Port,” put “3389” (assuming this is RDP). You will put this same port number in four times (again a range of only one port).
- Next, create a new policy under “Policy & Objects” -> “IPv4.” For “Incoming Interface,” select Port1.
- For “Source Address,” select “all.”
- For “Outgoing Interface,” select Port2.
- For “Destination Address,” select the name of the virtual IP that you created above.
- For “Service,” select RDP. Ensure that “Action” is set to “Allow” and “NAT” is on. You can turn on any additional security profiles you would like.

You must also have an Azure UDR in place in each subnet that sends traffic destined for any VPNs and the default route (0.0.0.0/0) to an internal address associated with the FortiGate (typically Port2). These can be created or configured within the Azure portal.

Again, in Microsoft Azure, IT cannot use a public IP associated with a VM behind a firewall within Azure, as Microsoft doesn’t allow routing of public IPs through a VNet in this way. Any public IP that you want to use must be associated with either the FortiGate or an Azure Load Balancer in front of it.

Also, the VMs within Azure aren’t aware of any associated public IPs. The “External IP” in a virtual IP configuration on FortiGate is the private (rfc1918) address of Port1.

Protect VM Images

Azure Virtual Machines provide the ability to create and manage the entirety of a VM. These VMs can be deployed from a library of images including varying versions or distributions of Windows Server. The VM golden image and template practices apply to Microsoft Azure deployment where customers should use these images only if they trust the suppliers. Securing the operating system of a VM requires roughly the same steps as securing a physical server. The security features provided by Windows Azure mainly reside at the network and infrastructure layer of the platform.

Common Security Topics for Windows Azure IaaS Virtual Machines

A Windows Azure IaaS Virtual Machine is the compute offering that places the most security responsibility in the hands of the tenant. Fortinet provides advanced security beyond the network

access controls from the Azure platform. It offer anti-malware/ antivirus, web application firewall, log analytics, updates from best-in-class security intelligence, and centralized management and visibility into all FortiGate appliances deployed.

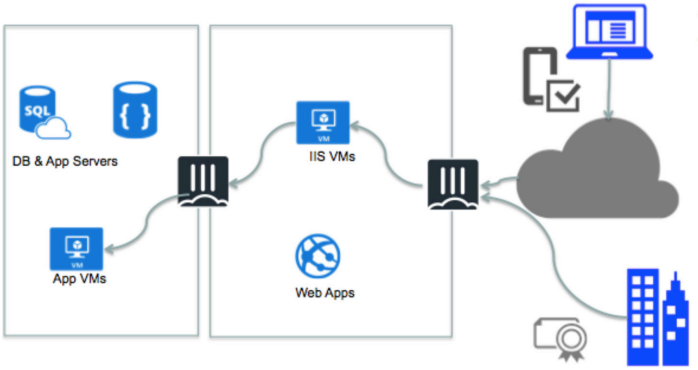
Securing Windows Azure Web Sites

Windows Azure Web Sites enables developers to quickly build, deploy, and run Web Sites in the scalable cloud environment. Developers can author Web Sites using ASP.NET, PHP, node.js, Python, or classic ASP and then publish their Web Sites using one of a number of standard publishing technologies.

Windows Azure Web Sites is a multi-tenant SaaS offering that is designed specifically for hosting web pages. Developers who are familiar working with web applications on IIS should find Windows Azure Web Sites to be a very similar experience.

Configuring Multi-tiered DMZs on Azure

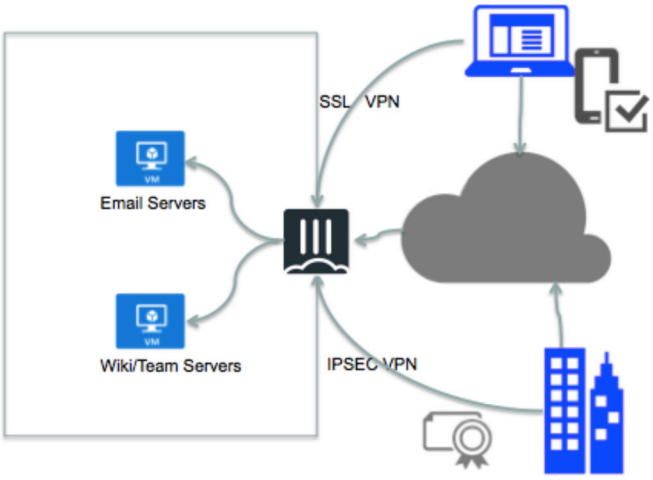
It is common to deploy applications in multiple tiers – web, app, and database. This covers ingress and egress, and intra-VM (VM-VM) traffic can be configured to the firewall. This configuration can be used to enhance DMZ security and isolated cloud networks.



To achieve this design, customers can manipulate VNet design and access with UDRs and Network Security Groups (NSGs). This design is not limited to two or three isolations. You can customize your FortiGate appliances per your own requirements. The solution provides full isolation with multi-NIC VM servers in the first tier.

Making Private Networks in the Public Cloud

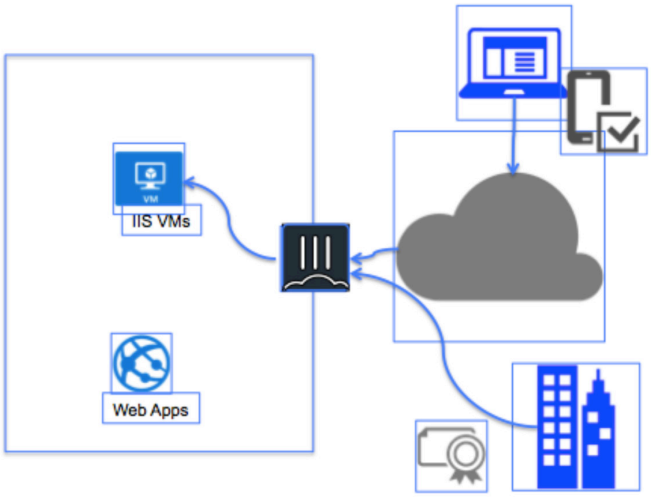
Microsoft Azure allows any organization to build their private network instantly without the limitations posed by current DMZ services. It helps reduce or eliminate local data centers, resulting in a decrease in CAPEX and an improvement in elasticity. With FortiGate enterprise-class IPS and application controls, your Azure cloud can be more secure than your data center. Placing FortiGate on the ingress and egress network path enables you to configure your IPsec and SSL VPNs within minutes.



Configuring Secured DMZs on Azure

Organizations that leverage the cloud for their public resources can take advantage of Microsoft's optimal placement of web resources. This helps maintain security with full NGFW enterprise security and IPS.

The FortiGate appliance can assist Layer 3 and Layer 4 network access control lists (ACLs). It helps deliver FortiGuard powered IPS and application controls to support both IPsec and SSL VPNs.



Globally Resilient Performance Optimization

Microsoft Azure Stack brings software-defined networking, pooling direct-attached storage, handling (and securing) virtual machines, and monitoring as a new private cloud solution. With the broader set of Fortinet VM support on leading hypervisors such as Windows and Linux distribution, customers can leverage from on-premise data center to the cloud with a globally resilient security design with performance.

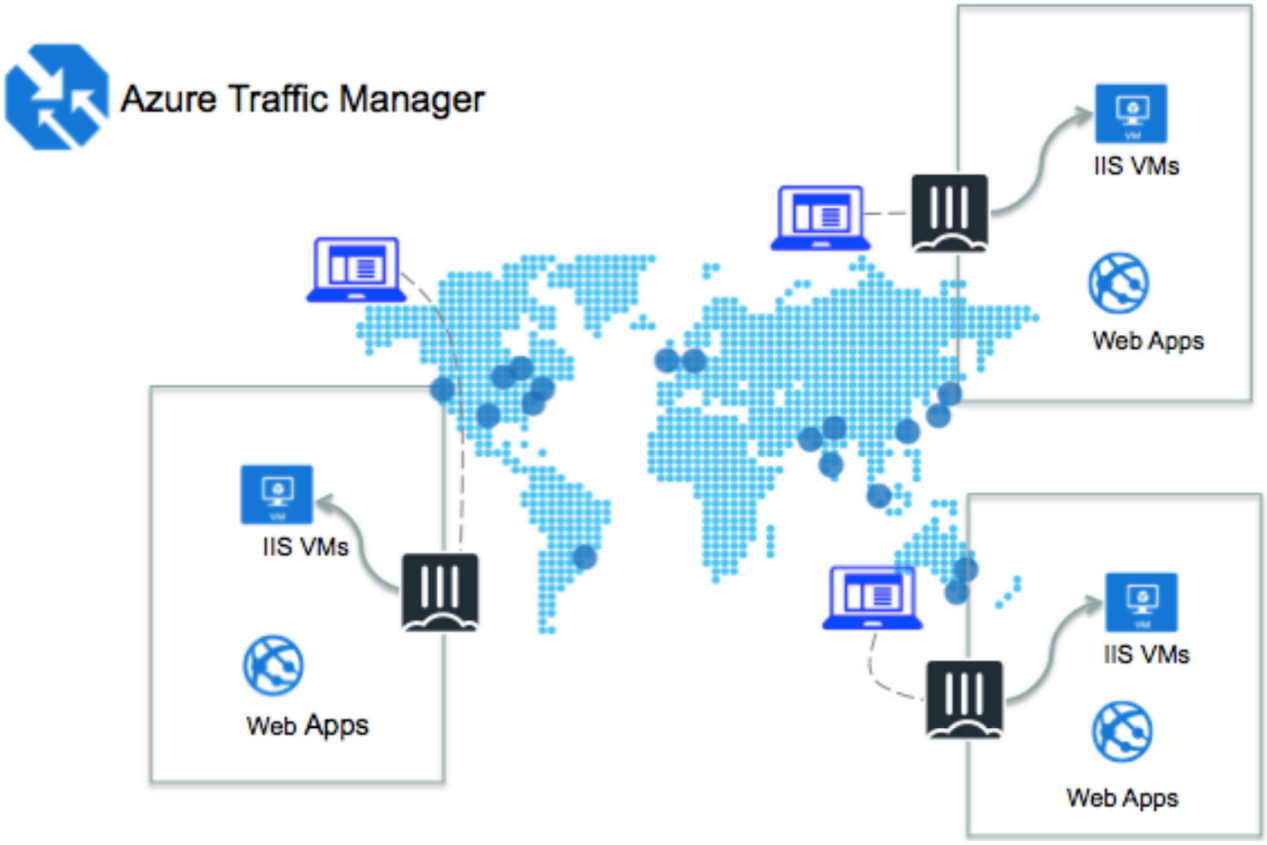
Microsoft Azure Service Fabric runs as micro-services on Azure Stack. DevOps can use the new Azure Resource Manager (ARM) to consistently deploy applications to either the public Azure cloud or to an Azure Stack data center. Fortinet provides GitHub access for ARM templates to ensure faster deployment.

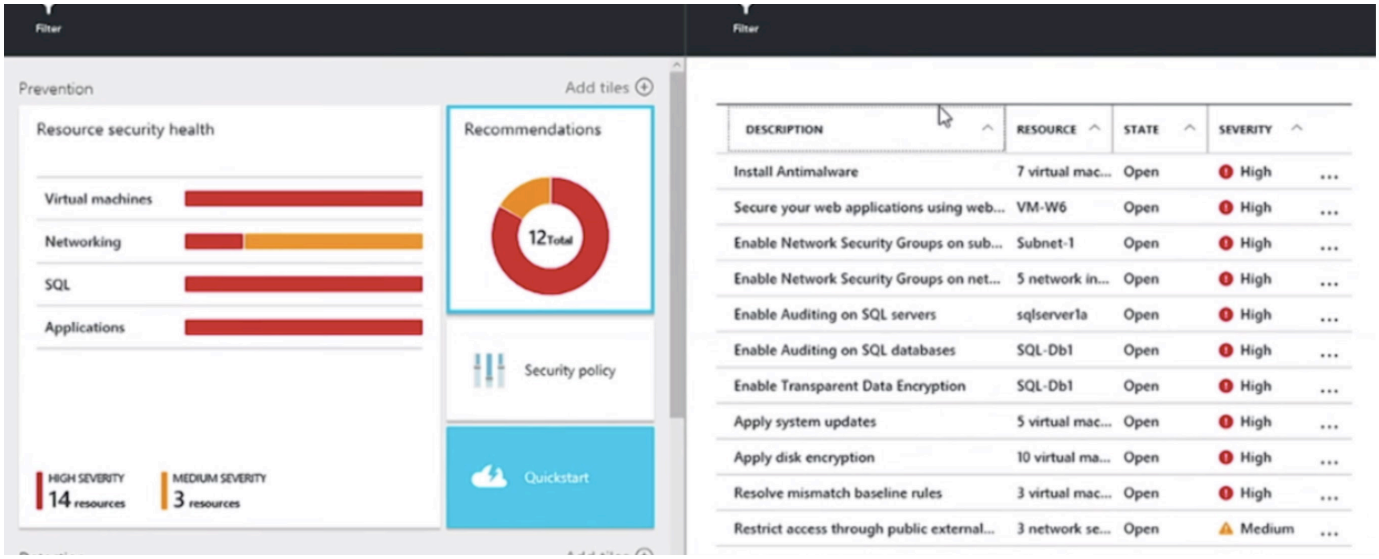
The beauty of the cloud is that any customer can turn on a cloud service globally with just a credit card and some cloud knowledge. Today, according to Microsoft, Azure is available in 140 countries, including China, and supports 10 languages and 24 currencies. For large enterprises, providing localized services that meet regional compliance is critical.

FortiGate in Azure supplies local access for customers and helps reduce latency. In particular, the high-availability design provides redundancy to ensure always-on services, a feature that is present on literally all Fortune 10 companies' must-have lists.

DevOps can deploy and integrate FortiGate appliances with Azure Traffic Manager for optimized load balancing. With the latest FortiOS 5.4.1, the compliance report on PCI DSS 3.x can be generated with just a few clicks. Compliance in the cloud is not just a manual snapshot. Instead, it's a continuously automated process with full control and visibility throughout global presences. FortiAnalyzer and FortiManager provide the centralized compliance visibility and consistent updated patches to ensure no silo exists or to get oversight during a global rollout.

In addition, FortiMail and FortiWeb can be used to protect Office 365, mail gateways, web applications, etc.





Azure Security Center (ASC) Recommendation

Fortinet is certified by Azure Security Center, which provides policy-driven monitoring of security policies. It scans through your current Azure deployment and provides recommendations for how to proactively prevent vulnerabilities or remediate threats that have occurred.

Summary

Fortinet Security Fabric for the cloud can prevent, detect, and respond to threats with increased visibility into and control over the security of your Azure resources. When you understand your cloud security state, your business can stay ahead of legacy or emerging cloud threats. With the open framework in the Fortinet Security Fabric, it's easy to combine Fortinet products with Microsoft Azure platforms and insights into cloud security-related events across your Azure deployments. For more information on detailed deployments and quick-start steps, please visit www.fortinet.com/azure or email azure@fortinet.com.

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
Valbonne
06560, Alpes-Maritimes,
France
Tel: +33.4.8987.0500

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

LATIN AMERICA SALES OFFICE
Paseo de la Reforma 412 piso 16
Col. Juarez
C.P. 06600
México D.F.
Tel: 011-52-(55) 5524-8428

August 5, 2016