SOLUTION BRIEF

Fortinet Cloud Services Hub in AWS

Executive Summary

When adopting any new cloud environment—such as Amazon Web Services (AWS)—organizations must balance the potential benefits of the cloud against their own ability to maintain effective security. Security can often be considered an inhibitor to productivity and agility as well as the organization's ability to develop new applications. Organizations can leverage the elasticity, availability, and scalability of AWS for building centralized security into an autonomous services hub that serves a variety of business needs. The broad set of security products that complement the Fortinet Security Fabric are ideal components in such an architecture. Concentrating security services helps organizations to maintain their obligation in the shared responsibility model of the cloud by protecting their data and assets stored in the cloud while ensuring consistent security policies across their entire infrastructure.

Effective security requires a consistent set of controls that are natively integrated into the cloud infrastructure and that provide broad protection and streamlined security management through automation.

Globally Available, Centrally Managed, and Scalable Security

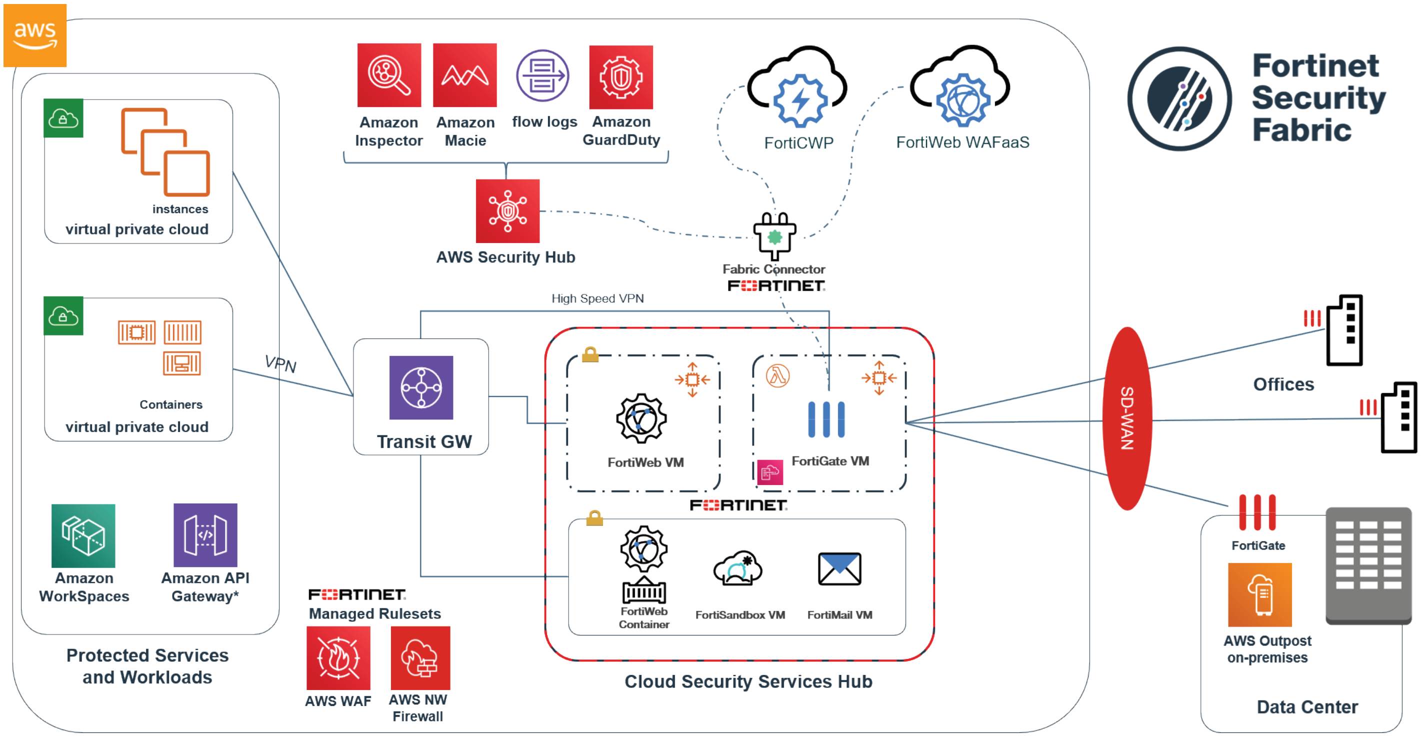
Effective security requires a consistent set of controls that are natively integrated into the cloud infrastructure and that provide broad protection and streamlined security management through automation. Establishing a cloud services hub that can share security services across the organization—including on-premises and in cloud environments—offers a superior approach for confident cloud adoption. There are several key use cases that illustrate the benefits:

1. Multiple remote branches. Branch connectivity can leverage a cloud services hub architecture to secure a variety of remote networking communication requirements. These include:

- Connecting from branch offices to specific protected resources that are hosted in the cloud, in cases where applications are built in the cloud. In this scenario, application security residing in the cloud and connected to branches and cloud resources offers the benefit of a single point of control and management for all cloud-based applications.
- Connecting through the cloud to private data centers via high-speed virtual private network (VPN) connections. Here, the cloud serves as the inbound point for internet-originating traffic by leveraging the global presence of the AWS cloud, with all traffic tunneled into private data centers and offices over high-speed, secure VPNs.
- Connecting out to the internet through the cloud, where the cloud scrubs traffic and performs the necessary security functionality needed to enable secure outbound connectivity without deploying costly devices in every location.

2. Multiple virtual private clouds (VPCs). This applies to situations where new applications are rapidly developed over the cloud and where different departments are responsible for different business applications. Some organizations need the highest possible flexibility to experiment with new technologies and to develop applications at their own pace. However, a lack of security within these mini-environments becomes a serious issue. The ability for different business units to simply connect their VPC into a cloud services hub offers the benefit of both worlds. Security can be centrally managed and enforced to manage the risks to the business without tethering the agility of organizational units by allowing them to operate freely.

3. Hybrid cloud. In a hybrid cloud deployment, large amounts of data are regularly transferred between on-premises locations and the cloud. Moreover, application components—which typically reside between the cloud and on-premises—must be able to operate at high speeds, regardless of where they are placed. A shared services hub architecture that can auto scale with fluctuating demands tremendously simplifies the design and operation of a hybrid cloud infrastructure. In cases where both the cloud and on-premises infrastructures are connected to the internet, this also provides a consistent set of security policies across locations for seamless management.



Distributing Security Via the Fortinet Cloud Services Hub in AWS

For AWS cloud users, Fortinet-enabled cloud services deliver a variety of security capabilities from a central location. These are integrated via the Fortinet Security Fabric. These services all leverage a cloud-native ability to automatically scale and replicate services in other regions. They include:

1. Next-Generation Firewall (NGFW) access control. Using a FortiGate NGFW, the cloud services hub enforces restrictions based on cloud resource tags, IP addresses, TCP services, and application control policies for both outgoing and incoming traffic.

2. VPN connectivity. The cloud services hub can also use FortiGate NGFWs to establish and maintain secure VPN cloud connectivity from branch offices, other data centers, office locations, remote users, or even from organizational VPCs residing in the cloud. This ensures that all traffic is transmitted confidentially over shared resources.

3. Secure web gateway. FortiGate can also be used as the exit point out to the internet for organizational offices, branches, or even backhauled remote users. In this configuration, the cloud services hub enforces acceptable internet usage policies for employees and mitigates the risk from malicious or suspicious communications.

4. Web application security. A FortiWeb web application firewall (WAF) can be used as the entry point for internet traffic accessing web-based applications. This allows for a central set of WAF security policies to protect business-critical applications from sophisticated attacks while ensuring compliance with regulatory requirements, such as the Payment Card Industry Data Security Standard (PCI DSS) and the Health Insurance Portability and Accountability Act (HIPAA).

5. Email security. When the cloud serves as the inbound internet gateway or where mail applications reside inside the cloud, FortiMail can be deployed on demand as a backup secure email gateway (SEG). This helps mitigate concerns about availability of different mail services and offers flexibility for global email deployments.

6. Sandboxing. Protecting cloud environments from zero-day attacks is growing increasingly important. As part of the cloud services hub, FortiSandbox sandboxing protection supports several use cases. It can integrate with the FortiGate to scan any in-line traffic. It can help protect applications leveraging the FortiSandbox JSON API. FortiSandbox can also scale to Amazon S3 cloud storage buckets via lambda functions. With the proliferation of collaboration tools and the increasing use of public file and image repositories, the ability to safely test suspicious code to expose new threats is more relevant than ever.

Cloud Connectivity Architectures and Services

Different use cases require specific design and deployment architectures. Fortinet's cloud services hub for AWS can leverage both the more common Transit VPC Architecture as well as the newer Transit Gateway Architecture. Both solutions allow the cloud services hub to seamlessly enforce security for cloud-based resources using native cloud metadata (e.g., tags, VPC IDs, instance IDs) and services such as configuration templates, auto scaling, and lambda Function-as-a-Service (FaaS) capabilities.

The **Transit VPC Architecture** is set up where all VPN termination is performed by FortiGate NGFWs. This includes VPN tunnels that are connected over the internet as well as VPN tunnels connected with other VPCs in the AWS cloud. In the case of the latter, the peer is an AWS VPN gateway. The Transit VPC solution offers high-speed VPN and the scalability for large deployments. However, it also requires more specific operational routines to support the infrastructure changes, such as additional VPCs being connected to the internet or the need to scale out the services hub. Subsequently, this also requires more expertise with Fortinet solutions.

The **Transit Gateway Architecture** simplifies deployment and allows for very simple operational routines to accommodate changes to the infrastructure as well as a deeper integration into the AWS cloud. However, it may be less suitable for organizations building a multi-cloud VPN-based infrastructure, due to some of the unique VPN implementations associated with the AWS cloud.

Centralized Security With Far-reaching Impact

An autonomous cloud services hub can extend the integrated defensive capabilities of the Fortinet Security Fabric from a central location out to the distributed ends of a modern enterprise organization. Using the elasticity of AWS to centralize and scale security services can help organizations protect their remote branches, VPCs, and hybrid cloud infrastructures. It concurrently helps ensure compliance with the latest data protection laws and industry regulations.

www.fortinet.com

May 9, 2021 11:30 PM

D:\Fortinet\Work\2021\0509\sb-forticare-cloud-services-hub-aws

928843-0-0-EN