DEPLOYING PERVASIVE SECURITY WITH AWS TRANSIT GATEWAY AND FORTINET CLOUD SERVICES HUB
EXECUTIVE SUMMARY

Most AWS deployments have evolved from a single virtual private cloud (VPC) to multiple VPCs spread across several regions. The Fortinet Transit VPC solution supports organizations that have storage and compute infrastructures spread across on-premises data centers and Amazon Web Services (AWS) VPCs. It enables them to not only interconnect globally distributed workloads but also to protect VPC environments with the advanced features of the Fortinet Security Fabric. With the launch of AWS’s highly scalable and distributed AWS Transit Gateway service, the Fortinet Cloud Services Hub can offer integrated capabilities to further extend Security Fabric protection. The Cloud Services Hub includes full auto-scaling capabilities as well as powerful routing and security features.

Until recently, if organizations wanted to interconnect their VPCs, they had limited options. They could create point-to-point peering to manage networking at each VPC (adding great complexity). Or, they could create IPsec tunnels from each VPC to third-party router/firewall appliances in a shared VPC. This results in a hub-and-spoke topology called “transit VPC.” While transit VPC deployments, such as Fortinet Transit VPC, have become a preferred approach to address inter-VPC connectivity and security requirements, an AWS Virtual Private Gateway (VGW)—deployed at each VPC spoke to terminate VPN connections—has serious bandwidth restrictions. This, in turn, limits network performance.

The AWS Transit Gateway resolves this issue through a new, highly scalable, distributed service that allows connectivity at scale. Since it supports equal-cost multi-path (ECMP) routing, traffic can be equally distributed over two or more VPN connections that propagate the same IP prefix. This allows for significantly more flexibility in the network. And because it is part of the AWS suite, native services such as CloudFormation, CloudWatch, and VPC Flow Logs can be used to manage and monitor the AWS Transit Gateway.

WHY TRANSIT GATEWAY WITH FORTINET CLOUD SERVICES HUB

The Fortinet Cloud Services Hub offers an exceptionally high value proposition for helping to secure AWS Transit Gateway deployments. Key benefits include:

DEPLOYMENT AT SCALE

The Fortinet FortiGate Next-Generation Firewall (NGFW) is uniquely positioned to offer rich security and routing capabilities to customers. It supports a range of performance requirements via its large pool of supported Amazon Elastic Compute Cloud (EC2) instance sizes—from as few as a single vCPU to instances with as many as 36 vCPUs. In addition, FortiGate NGFWs integrate with AWS Auto Scaling, thereby allowing organizations to dynamically scale up or down routing and security capacities based on predefined metrics such as network congestion and CPU utilization.
NETWORK DESIGN FLEXIBILITY

Although AWS Transit Gateway can connect to on-premises physical or virtual VPN appliances, many organizations prefer to maintain their existing networking posture. Fortinet Cloud Services Hub is designed to accommodate those needs—as well as organizations that wish to connect their on-premises devices directly to AWS Transit Gateway.

INTEGRATION WITH NATIVE AWS SERVICES

The Fortinet Cloud Services Hub leverages the monitoring and managing features of several AWS services, including Transit Gateway, Auto Scaling Lifecycle Hooks, CloudWatch, and Serverless Lambda Functions, to offer a robust Transit Network solution.

ZERO-TOUCH PROVISIONING

Fully automated, end-to-end, multi-cloud deployments at scale utilize key AWS automation tools such as CloudFormation and Lambda Functions to provision necessary configurations to virtual and physical devices in the network. AWS CloudWatch also reads auto-scaling events that trigger desired actions.

ADVANCED SECURITY

Fortinet FortiGate NGFWs include advanced security capabilities like threat protection, SSL inspection, and ultralow latency for protecting critical environments from known and unknown attacks. As a core part of the Fortinet Security Fabric, it also integrates with other key security technologies in real time, such as zero-day malware detection.

SINGLE-PANE-OF-GLASS MANAGEMENT

The Fortinet management platform provides a single pane of glass across the entire Fortinet Security Fabric, regardless of the location or the form factor of the managed devices. This minimizes the operational complexity of hybrid cloud environments utilizing the Fortinet Transit Network offering.

CONSISTENT SECURITY POLICIES

A Fortinet Fabric Connector can allow the Fortinet Cloud Services Hub to apply firewall policies automatically. All dynamic address groups across different platforms can be synchronized. This ensures that policies are enforced consistently across on-premises and AWS deployments (as well as other supported platforms).
HIGH AVAILABILITY

FortiGate NGFWs in the internet-facing VPC are deployed in at least two distinct availability zones. This helps increase service resiliency.

USE CASES: FORTINET CLOUD SERVICES HUB AND AWS TRANSIT GATEWAY

The Fortinet Cloud Services Hub leverages the AWS Transit Gateway service to enable and improve upon several critical use cases. These include:

CLOUD-ONLY DEPLOYMENT WITH AUTO SCALING AND ECMP

Since many AWS customers have their workloads spread across multiple VPCs, it is of utmost importance to allow inter-VPC connectivity while scaling FortiGate capacities based on network traffic. This allows for a fully scalable and cost-effective solution. In this deployment, application VPCs (often referred to as “spoke VPCs”) attach to the AWS Transit Gateway via Transit Gateway attachment objects. The AWS CloudWatch service is used to trigger Lambda Functions once it is notified of a lifecycle change event. As new FortiGate instances are spawned by the Auto Scaling Group, IPsec tunnels are dynamically and automatically created using the ECMP feature. This allows for equal distribution of traffic across all tunnels.

HYBRID CLOUD (MULTIPLE VPCS AND MULTIPLE REMOTE SITES WITH AUTO SCALING AND ECMP)

In a typical hybrid cloud deployment, a large volume of data is continuously transferred between multiple remote branches, the corporate data center, as well as application VPCs. In a nutshell, the Fortinet Cloud Services Hub creates a central hub VPC in the cloud to facilitate interconnectivity and traffic inspection. While application VPCs attach directly to the Transit Gateway, physical data center and remote branch locations can connect to the FortiGate NGFW in the Fortinet Cloud Services Hub using ECMP in a scalable fashion. Additionally, this deployment model gives organizations more flexibility, in that they do not need to change their overall network design and internal team responsibilities.

EAST-WEST TRAFFIC INSPECTION

As zero-trust security deployment strategies are adopted by large and small enterprises, the ability to inspect all traffic is critical. Recent studies show that the vast majority of multi-cloud traffic travels laterally (east-west) across the environment. The Fortinet Cloud Services Hub supports a deployment model where all traffic is inspected to stop the lateral propagation of threats.
This can be achieved in two different ways:

- **Deploy FortiGate NGFWs at each application VPC.**
  Deploying a FortiGate solution at each VPC allows security policies to be enforced at the individual VPC level, while also enabling east-west traffic inspection. And as with FortiGate NGFWs deployed in the Fortinet Cloud Services Hub, the spoke VPC FortiGate solutions also connect to the Transit Gateway through IPsec tunnels.

- **Create multiple route tables in the AWS Transit Gateway.**
  This approach allows all or a subset of inter-VPC traffic to be inspected by the advanced security capabilities in FortiGate (and, by extension, potentially other security solutions across the Security Fabric). All traffic that needs to be inspected is sent to the FortiGate solutions deployed in the Fortinet Cloud Services Hub. As shown in Figure 2, two Transit Gateway route domains are used in this deployment: one route table that attaches to all spoke VPCs and another one that attaches to the Cloud Services Hub VPC. To ensure flow affinity, source NAT has to be applied at each FortiGate NGFW. Additionally, each spoke VPC route table must have a route back to the Cloud Services Hub.

**INBOUND APPLICATION TRAFFIC WITH FIREWALL RESILIENCY**

Many customers prefer to deploy their applications in private subnets in VPCs that do not require any public IP addresses. Yet, the need to protect applications from outside attacks does not go away. Because the Fortinet Cloud Services Hub integrates with the AWS Transit Gateway, customers can conveniently deploy web applications in a private VPC while resilient FortiGate NGFWs are provisioned in a public VPC to protect their applications.

Figure 3 depicts a scenario where a FortiGate NGFW is deployed in an Auto Scaling Group fronted by an internet-facing AWS load balancer. A web server is also deployed in a spoke VPC that connects to a Transit Gateway. When a remote client contacts the web server, the following sequence of events occurs:

- The end user sends a URL request, which is resolved by a DNS server (possibly Route 53). In this example, the URL is resolved to the IP address of the public load balancer.
- The load balancer sends traffic to its target group—the FortiGate Auto Scaling Group (which has two instances in the Figure 3 example). This translates the packet’s destination IP address to the IP address of the public-facing interface (ENI-1) of one of the FortiGate NGFWs. Also, to ensure that the traffic returns to it on the reverse flow, the load balancer translates the source IP address of the packet to its own private IP address.
- The FortiGate NGFW will then translate the source IP address of the packet arriving at its ENI-1 interface to the source IP address of its ENI-2 interface. Additionally, the packet’s destination IP address is translated to the IP address of the web server.

Therefore, both destination network address translation (DNAT) and source network address translation (SNAT) are performed by the firewall at this stage.
WEB APPLICATION FIREWALL (WAF) VPC FOR MULTIPLE APPLICATIONS

- Combining the Transit Gateway with the Auto Scaling Group allows organizations to deploy a resilient and scalable WAF to protect multiple application VPCs. Similar to the first use case, the AWS Auto Scaling Group, CloudWatch, and other services are used to dynamically scale WAF capacity up or down to meet changing traffic volume requirements.

The Fortinet Cloud Services Hub protects workloads in a dynamic, scalable, and automated manner.

COMBINED FORCES FOR SCALABLE AND SECURE MULTI-VPC DEPLOYMENTS

The Fortinet Cloud Services Hub protects workloads in a dynamic, scalable, and automated manner. This enables compute and storage infrastructures to be spread across multi-account, cross-region VPCs as well as physical data centers and remote locations. The combination of the AWS Transit Gateway service and the Fortinet Cloud Services Hub allows for even more scalable security.

Taking advantage of FortiGate NGFWs, FortiWeb WAFs, and AWS-native services such as Lambda, CloudWatch, and Auto Scaling Group, the Fortinet Cloud Services Hub can address many more use cases. These include east-west and north-south traffic inspection, inbound application traffic with firewall resiliency, and a WAF deployed in a shared VPC to protect multiple applications.