Enterprise Strategy Group by TechTarget

Technical Validation

Fortinet FortiGate Cloud-Native Firewall Service on Amazon Web Services

Implementing Cloud-based Workload Security with Minimal Overhead

By Alex Arcilla, Senior Validation Analyst

December 2022

Introduction

This Technical Validation from TechTarget's Enterprise Strategy Group (ESG) documents our evaluation of the Fortinet FortiGate Cloud-Native Firewall (FortiGate CNF) Service on Amazon Web Services (AWS). We reviewed how this product can help organizations to ensure that network security is enforced throughout a cloud-based network with consistent policies without the overhead of deploying and managing individual firewalls deployed throughout an organization's public cloud infrastructure.

Background

Enterprise Strategy Group (ESG) research uncovered that a majority (55%) of respondents' workloads run on public cloud infrastructure-as-a-service (IaaS) today. This is expected to grow to nearly two thirds of workloads (62%) over the next 24 months.[1]

Unfortunately, most organizations (88%) report challenges securing their IaaS environments. While ESG research uncovered that the threat landscape continues to pose the biggest challenge (52%), survey respondents also cited an increase in the amount of IaaS usage (39%), the lack of the right level of IaaS security skills (30%), and the lack of the right level of IaaS security staff (28%).[2]

Figure 1. Top 5 Public Cloud Security Challenges

Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Meeting business needs quickly can be difficult when attempting to secure public cloud-based workloads using traditional firewalls and related workflows. Often, organizations cannot Incorporate the appropriate level of security that typically exists in their on-premises workloads, having to balance ease of use with "best-in-class" security.

The range of products and services available from third-party security vendors and cloud service providers (CSPs) does not make securing these workloads any easier. While the boundary of any cloud-based network is dynamic and scales as business needs dictate, third-party solutions have not been designed to scale as flexibly, translating into additional IT overhead and expenses for additional deployment, configuration, and policy management efforts. At the same time, CSP-specific firewalls may not possess the functionality that organizations need to build the level of network security they are

[1] Source: Enterprise Strategy Group, Complete Survey Results, *Network Security Trends in Hybrid Cloud Environments,* December 2021.
[2] Ibid.

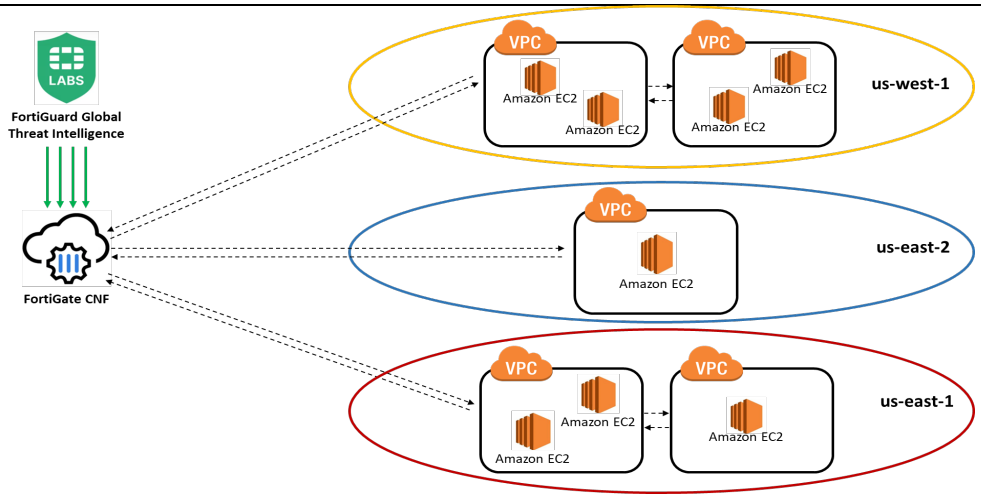
accustomed to within their on-premises networks. To complicate matters further, the continuing gap in IaaS security skills highlights the need for a solution that is easy to implement yet does not compromise overall network security.

FortiGate CNF on Amazon Web Services

The FortiGate CNF Service has been designed to help organizations eliminate the burden of managing the underlying scalability and availability of a network security infrastructure on AWS. As a managed firewall-as-a-service (FWaaS), FortiGate CNF provides and scales advanced Layer-7 protection as organizations scale the number of Amazon virtual private clouds (VPCs) supporting workloads. It inspects and protects outbound, inbound, and east-west (VPC-to-VPC) network traffic.

With FortiGate CNF Service on AWS, organizations can deploy and operate consistent network security policies for traffic traversing across its Amazon VPCs.[3] Unlike relying on workload-specific inspection and filtering policies deployed only at the firewall, organizations using FortiGate CNF associate policies with an AWS workload's metadata tags, such as Amazon EC2 instance ID or type. Should any workload migrate or scale to other Amazon VPCs, FortiGate CNF ensures that the workload is governed by the same security policies. The need to reconfigure policies on individual firewalls as traffic patterns change is eliminated. In addition, organizations can ensure that traffic into, out of, and between Amazon VPCs is secured, without incurring the operational overhead of deploying individual virtual firewalls at every Amazon VPC.

Figure 2. FortiGate CNF



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

To simplify security operations, FortiGate CNF integrates with AWS Gateway Load Balancer to reduce the effort related to managing network routing, as well as to automate scaling as the number of Amazon VPCs changes. FortiGate CNF also integrates with AWS Firewall Manager to simplify security management and automate security rollout.

In addition, Fortinet ensures that FortiGate CNF Service on AWS remains current with multiple security signatures and IP reputation information, supplied by FortiGuard Services, so that organizations can keep policies up to date without the need to continually refresh this information.

While FortiGate CNF is a managed service, organizations with hybrid cloud environments that include AWS can also manage this service via FortiManager, enabling automated, centralized, and consistent security management across AWS and on-premises deployments uniformly, as well as other FortiGate form factors (physical and virtual).

[3] FortiGate CNF is available in the following AWS regions at the time of report publication: US East (N. Virginia), US East (Ohio), US West (N. California), US West (Oregon), Asia Pacific (Tokyo), Europe (Frankfurt), and Europe (Ireland).

Payment for use of the FortiGate CNF is based on a consumption model. Organizations only pay for the time their cloud-based network firewall instances are operational and for the amount of traffic processed by those firewall instances. Annual payment options are also available.

By leveraging the FortiGate CNF, organizations can avoid incurring the manual overhead and operational expenses related to managing their own network security infrastructure or deploying consistent security policies on AWS. More importantly, organizations embed the level of network security in their AWS-based networks that organizations are accustomed to seeing in their workloads running on-premises.

Enterprise Strategy Group Technical Validation

We evaluated the FortiGate CNF Service on AWS via remote product demonstrations conducted at Fortinet's headquarters in Sunnyvale, CA. Testing was designed to review how FortiGate CNF can help organizations simplify deployment of a firewall infrastructure and apply consistent inspection and filtering policies for workload traffic.

Simplify Deployment

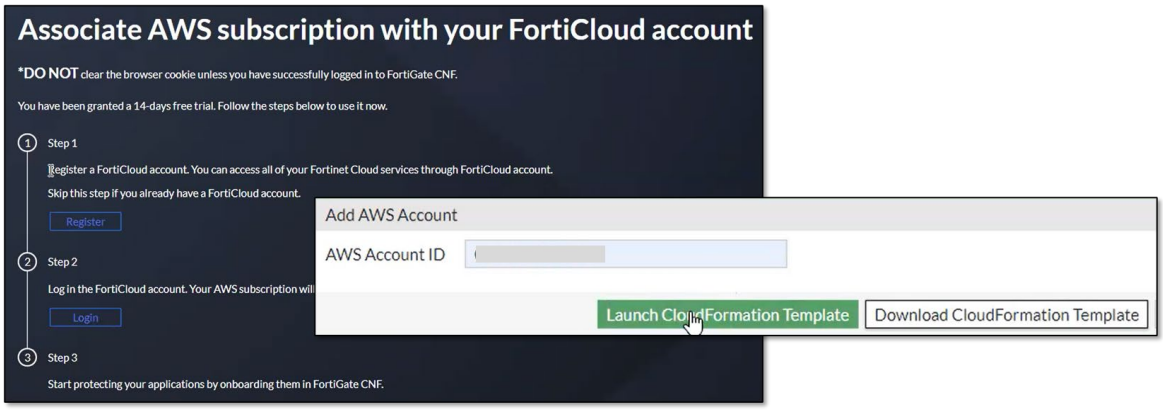
Deploying and updating multiple firewalls—third party or CSP-specific—to inspect and filter workload traffic traversing multiple Amazon VPCs can easily incur unwanted operational overhead and expenses. Should the workload scale, requiring more AWS resources, or migrate to other AWS resources, organizations either have to reconfigure existing firewalls or deploy new ones, incurring both operational overhead and expenses.

With the FortiGate CNF Service on AWS, organizations simply direct select workload traffic to a FortiGate CNF instance for inspection and filtering. Once policies are applied, allowed workload traffic is directed to its destination according to the routing rules associated with the instance.

Enterprise Strategy Group Testing

Enterprise Strategy Group (ESG) first created a FortiGate CNF instance using AWS account credentials. (A single instance can support multiple AWS availability zones (AZs) and Amazon VPCs in an AWS region across multiple AWS accounts.) We ensured that an existing AWS subscription was associated with an existing FortiCloud account from the AWS interface before deploying the FortiGate CNF for this specific account. We then launched an AWS CloudFormation template to install the required software components to create and manage FortiGate CNF instances (see Figure 3).

Figure 3. Adding AWS Account ID to Existing FortiCloud Account

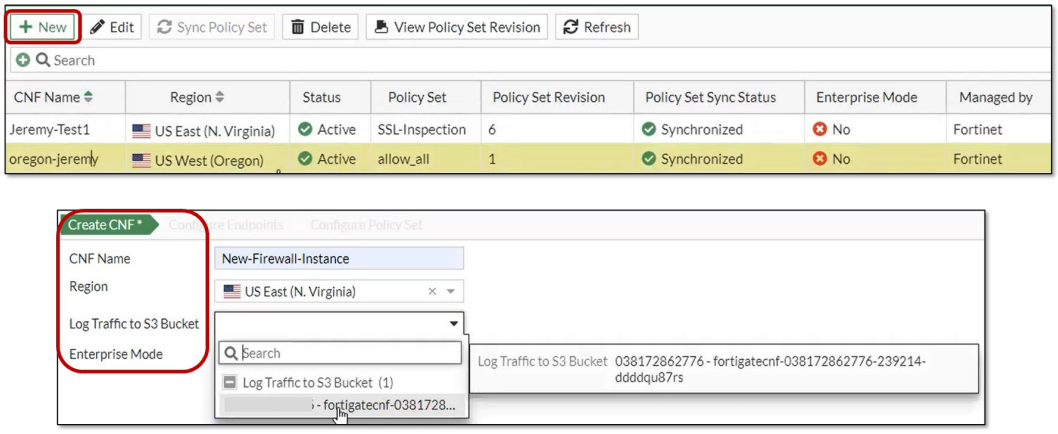


Source: Enterprise Strategy Group, a division of TechTarget, Inc.

We then created a new FortiGate CNF instance, to which traffic from specific workloads of an individual AWS account was routed before being sent to defined destinations. From the *CNF Instances* tab, we clicked on the "New" button, then filled in the name and chose the AWS region and Amazon VPC in which the instance would reside and the Amazon Simple

Storage Service (S3) bucket that would collect security logs (see Figure 4). We noted the option to choose "Enterprise Mode," which enables FortiManager to manage the CNF instance. Otherwise, FortiGate CNF Console, the same tool to create the CNF instance, is used.

Figure 4. Creating a FortiGate CNF Instance

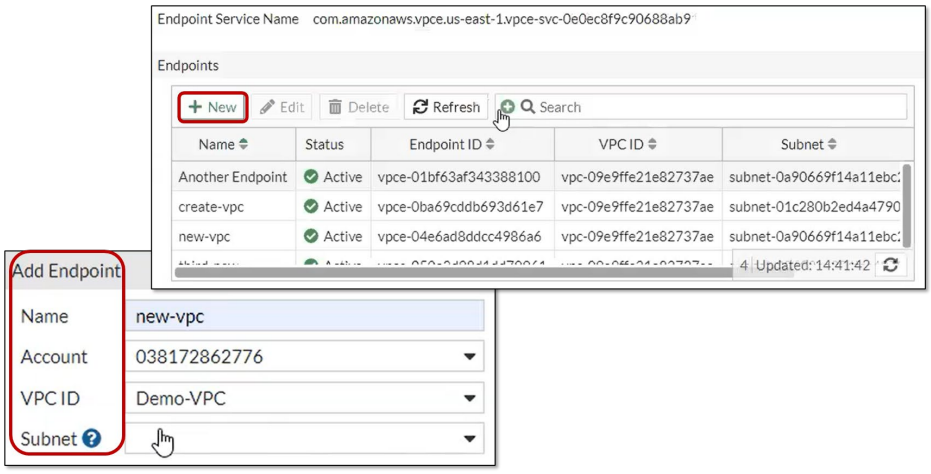


Source: Enterprise Strategy Group, a division of TechTarget, Inc.

To direct workload traffic through the FortiGate CNF, ESG assigned endpoints, subnets of a specific Amazon VPC, that represented the traffic's destination. From the webpage displaying existing endpoints in our AWS account, we clicked on the "**New**" button to add a new endpoint by specifying both the Amazon VPC ID and the subnet. We noted how this approach can simplify security infrastructure deployment and operations. Instead of installing individual virtual firewalls into multiple Amazon VPCs, traffic from multiple workloads can be directed to a single CNF instance before it is routed to specific subnets within selected Amazon VPCs.

Should a new compute instance be created within an existing subnet associated with a specific CNF, the CNF's existing policies are applied automatically. ESG noted how this approach can greatly reduce the effort to reconfigure firewalls when workloads scale.

Figure 5. Adding Endpoints to the FortiGate CNF

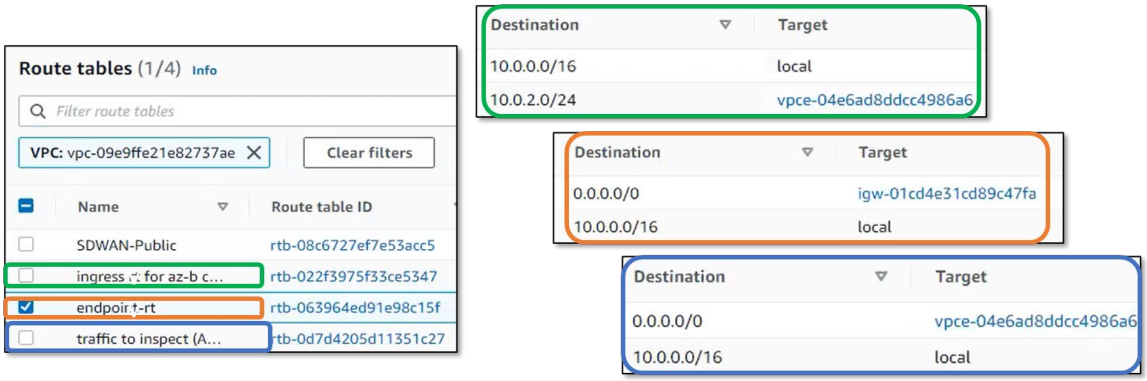


Source: Enterprise Strategy Group, a division of TechTarget, Inc.

To clarify how traffic is routed through a FortiGate CNF, ESG examined route tables associated with traffic destined for a specific endpoint, identified using metadata associated with the related Amazon VPC ID (see Figure 6). The following routes have been defined to enable inspection of bidirectional traffic by the FortiGate CNF.

- Orange box – send all traffic to the internet after traversing the internet gateway with the given ID, except traffic destined for the Amazon VPC with IP address 10.0.0.0/16.
- Blue box – direct all workload traffic to the endpoint, except traffic destined for the Amazon VPC with IP address 10.0.0.0/16.
- Green box – send ingress workload traffic to the endpoint first before routing to the Amazon VPC subnet.

Figure 6. Viewing Traffic Routes Into and Out of an Endpoint from Amazon EC2 Interface



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

We should note that these route tables were automatically created when adding new endpoints. No manual configuration of any endpoint's route table took place to direct how traffic is routed. This also helps to decrease deployment and configuration overhead, as well as to reduce any configuration errors that can potentially compromise an organization's security posture.

Why This Matters

Securing workload traffic traversing a cloud-based network of Amazon VPCs cannot be done by simply deploying and configuring firewalls at multiple points of entry, as is typically done with an on-premises network. While organizations can easily scale workloads up or down with AWS, the network perimeter is no longer fixed, requiring firewalls to be re-deployed and re-configured. Unfortunately, this approach incurs unwanted overhead and expense.

Enterprise Strategy Group (ESG) validated that the Fortinet FortiGate CNF Service on AWS can help organizations reduce the capital and operational expenses associated with deploying multiple firewalls within an AWS-based network. We observed the ease of creating a CNF instance to filter and inspect traffic from multiple workloads. ESG also reviewed how we can direct traffic inspected and filtered by the FortiGate CNF to specific Amazon VPCs and its subnets via endpoints, removing the need to deploy and configure individual firewalls at each Amazon VPC.

Apply Policies Consistently to Application Workloads

Ensuring that an organization's security posture is maintained requires that security policies are applied consistently to workload traffic. However, updating workload policies on virtual firewalls deployed in Amazon VPCs as instances are created or taken down or as workloads migrate to instances residing on other Amazon VPCs can consume time and effort unnecessarily, while overall network security is put at risk.

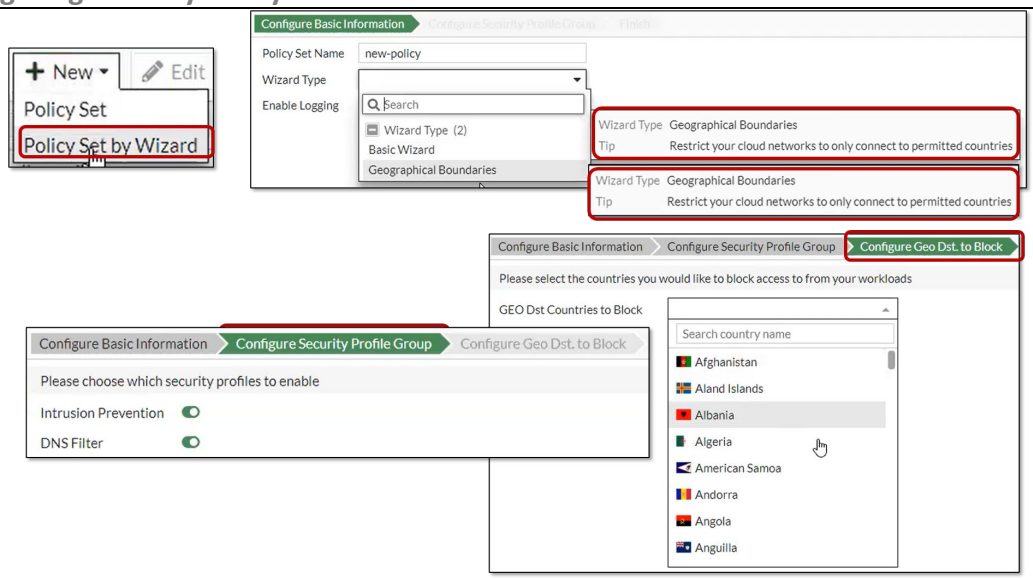
With the FortiGate CNF Service on AWS, organizations define and apply inspection and filtering policies according to the metadata tags associated with instances supporting specific workloads. Should workload instances scale up or down due to business demands, FortiGate CNF still applies policies consistently, as the policies are not exclusively coupled with the firewall. If the endpoints of a given workload change, only the endpoints associated with a FortiGate CNF instance have to

be updated. Organizations no longer need to update firewalls in multiple Amazon VPCs should the number or location of workload instances change.

Enterprise Strategy Group Testing

Enterprise Strategy Group (ESG) examined the ease of defining a policy set first. From the "**Policy Sets**" tab on the main menu, we opted to use a wizard (see Figure 7). We began with the "**Basic Wizard**" option to configure a security policy group that addressed intrusion prevention and DNS filtering. We could also create a policy set that blocked traffic according to the country of origin using the "**Geographical Boundaries**" option, in addition to intrusion prevention and DNS filtering.

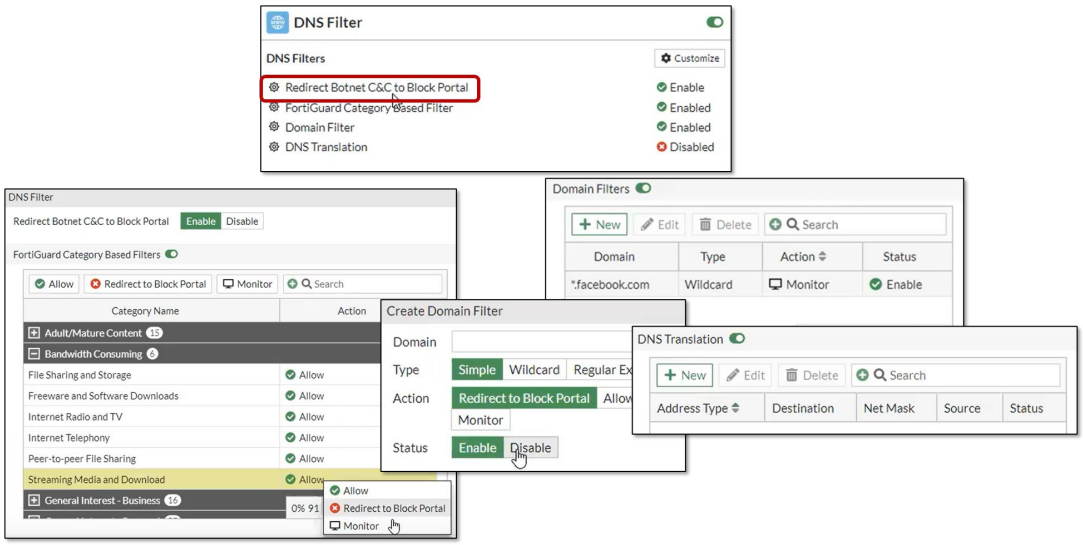
Figure 7. Configuring Security Policy Sets



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

To refine the DNS filtering rules, ESG observed how to customize these rules using data such as categories supplied by FortiGuard Services (i.e., collected IP addresses associated with specific subject material), specific domains (e.g., Facebook), customer domains (e.g., allowing updates from SaaS applications), or DNS translations (see Figure 8).

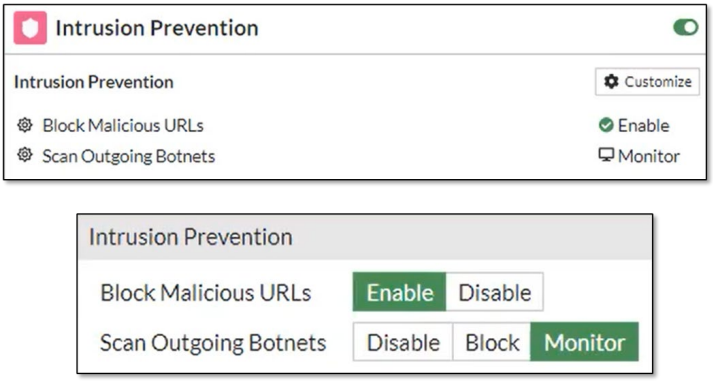
Figure 8. Configuring DNS Filtering Rules



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

We also reviewed the simplicity of customizing intrusion prevention rules. While the options were limited for dealing with malicious URLs and outgoing botnets (see Figure 9), we noted that FortiGuard Services continually updates IP addresses and signatures associated with these two categories.

Figure 9. Configuring Intrusion Prevention Rules

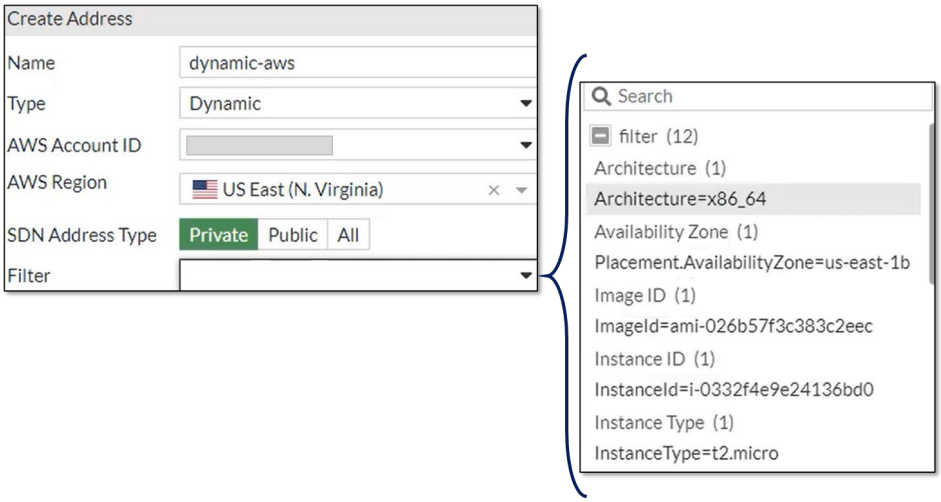


Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Since Fortinet has assumed responsibility for categorizing IP addresses, URLs, and domain names, as well as tracking malicious URLs and botnets, ESG could see how this helps to simplify security operations without risking an organization's security posture. Organizations do not need to track every IP address or domain name to decide what is to be allowed, blocked, or monitored. Using the categories compiled by FortiGuard Services eliminates the need for security operations to update firewall rules every time an IP address or domain name is deemed suspect. Less downtime incurred for updating firewall rules translates into decreased overhead and security risk.

Finally, ESG examined how FortiGate CNF can simplify the way these policy sets are applied to specific workloads. Leveraging the knowledge that a security policy is assigned to a specific workload using its AWS metadata tags, we observed how a policy set could be applied to multiple workloads with the same metadata tags. We navigated to the "Address" webpage of the FortiGate CNF interface and created a new dynamic-based address associated with a specific FortiGate CNF (see Figure 10). The address, named "dynamic-aws," would be associated with a specific AWS account ID and would apply to the account's resources in the AWS US-East region. Those workloads with private IP addresses and the chosen AWS metadata tags would be subject to the policies loaded onto this specific FortiGate CNF instance.

Figure 10. Configuring How Policies Are Applied to Individual Workloads



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Using this approach, ESG observed how this further helps to simplify security operations, as additional firewall rules do not need to be added to apply security policies to individual workloads. Instead, we saw how assigning the appropriate filters to the address ensures that the FortiGate CNF only applies the relevant policy set to only those workloads with the specified characteristics.

Why This Matters

Creating and applying security policies is necessary to filter and block malicious traffic but updating firewalls with rules tailored to individual workloads can be tedious, time-consuming, and error prone, especially when an existing policy can be applied to multiple workloads. On top of that, filtering and blocking traffic related to categories deemed as security risks (e.g., streaming video, social media) must be continuously tracked so that the relevant IP addresses are included. Unfortunately, tracking such data and updating the relevant firewall rules are tasks that are never completed.

Enterprise Strategy Group (ESG) validated that the Fortinet FortiGate CNF Service on AWS simplifies the creation and application of security policies across all workloads. We observed that we can create policy sets leveraging the research completed by FortiGuard Services, which supplies categories of IP addresses that organizations would typically want to block or monitor. Using these categories can reduce the time and effort organizations spend on setting security policies. ESG also verified that FortiGate CNF simplifies how organizations apply security policies to multiple workloads by filtering on characteristics of AWS-specific workloads, removing the need to update policies on individual workloads.

The Bigger Truth

Maintaining security policies on multiple virtual firewalls in an AWS-based network consumes time and effort. Whether using a third-party solution or the AWS firewall, the approach has been the same—deploying firewalls to inspect and filter traffic into, out of, and between Amazon VPCs. However, the overhead and expenses to deploy, configure, and manage these virtual firewalls can easily accrue. Further complicating this issue is the fact that as workloads scale or migrate to other Amazon VPCs, scaling firewall resources is not as flexible and straightforward as scaling AWS resources. Virtual firewalls have to be re-deployed and reconfigured. Policies used by those firewalls also need to be modified to accommodate new traffic patterns. And keeping policies updated to address newly discovered threats also consumes time and effort that take attention away from reinforcing an organization's security posture.

The Fortinet FortiGate CNF Service on AWS can help organizations address these challenges. This FWaaS has been designed to simplify the deployment, configuration, and management of a cloud-based security infrastructure. Instead of deploying and configuring multiple virtual firewalls into each Amazon VPC, organizations can deploy FortiGate CNF instances that filter traffic going into, out of, and between multiple Amazon VPCs. Rather than configuring policies for inspecting and filtering traffic of individual workloads, the FortiGate CNF enforces policies that are attached to each workload via AWS-related metadata tags. Thus, no matter where the workload resides, the policies remain consistent. With the FortiGate CNF Service on AWS, organizations can minimize the time, effort, and expense spent on ensuring its AWS-based network security, thus decreasing overall security risk.

Throughout our evaluation of the FortiGate CNF Service on AWS, Enterprise Strategy Group (ESG) validated that organizations can minimize operational overhead and costs, without sacrificing their AWS-based network security posture. We specifically validated how FortiGate CNF can:

- Simplify deployment of a virtual network security infrastructure that inspects and filters traffic of multiple workloads into, out of, and between Amazon VPCs, removing the need to deploy virtual firewalls in every Amazon VPC.

- Apply security policies consistently to workloads, especially in cases in which the workload scales or migrates to other Amazon VPCs, by ensuring that policies are tagged to individual workloads, eliminating the need to configure and update multiple policies for individual workloads on any given virtual firewall.

If your organization needs to secure workloads carried by an AWS-based network but does not want the burden of deploying, configuring, and updating multiple workload policies on multiple virtual firewalls, ESG suggests closely examining the Fortinet FortiGate CNF on AWS.

The goal of Enterprise Strategy Group (ESG) Validation reports is to educate IT professionals about information technology solutions for companies of all types and sizes. ESG Validation reports are not meant to replace the evaluation process that should be conducted before making purchasing decisions, but rather to provide insight into these emerging technologies. Our objectives are to explore some of the more valuable features and functions of IT solutions, show how they can be used to solve real customer problems, and identify any areas needing improvement. The ESG Validation Team's expert third-party perspective is based on our own hands-on testing as well as on interviews with customers who use these products in production environments.

Enterprise Strategy Group by TechTarget

Enterprise Strategy Group is an integrated technology analysis, research, and strategy firm that provides market intelligence, actionable insight, and go-to-market content services to the global IT community.

www.esg-global.com contact@esg-global.com 508.482.0188