CASE STUDY

Automating Fortinet Solution Rollouts in AWS Improves Efficiency, Reduces Risk of Human Error

When companies in the homeland security, healthcare, or manufacturing sector need sophisticated electronic components, they turn to OSI Systems, Inc. The company designs and manufactures specialized devices for functions ranging from diagnostic cardiology to freight cargo screening to photodiode sensors, then delivers these capabilities to clients as turnkey solutions.

An OSI subsidiary, S2 Global, is responsible for the hardware and software environments that clients require for their OSI solutions. "So, for example, if an order requires a rack with hardware inside, we build the rack, we set up the virtual machines [VMs], and we install the operating systems," explains Nikolay Chigrin, senior system engineer, AWS, for S2 Global. "Then we configure it and ship it to the client."

Some client projects include cloud-based applications. S2 Global provides essentially the same services for those projects. "With Amazon Web Services [AWS], we create the networking, spin up virtual machines in AWS, and configure everything," Chigrin says. "We do all the work, and the client just needs to connect to their VMs." After the initial configuration, "if something goes wrong, it is our responsibility to fix it," he says.

Because OSI clients require a high level of security for their data and applications, S2 Global has long used FortiGate next-generation firewalls (NGFWs) to secure the client environments it deploys. For implementations in AWS, S2 Global rolls out FortiGate VM to protect customers' virtual private cloud (VPC) environments.

"The FortiGate VM firewalls give us the capability to filter outbound traffic," Chigrin says. "Our clients are governments and big corporations, which have strict data protection requirements. All traffic to and from AWS is connected through VPN [virtual private network] tunnels, or traffic is allowed to visit only a whitelisted set of internet protocol [IP] addresses. That helps us control the client's vulnerabilities."

Standardization Enables Automation in NGFW Configuration

When Chigrin started with S2 Global 11 months ago, he saw an opportunity to streamline the deployment of FortiGate VM firewalls. Spinning up a firewall in AWS required hours of manual effort, some of which was unnecessary. Chigrin realized that standardizing portions of the firewall configuration would improve efficiency of both deployment and maintenance of the NGFWs.

"With our new automated setup, we just upload the FortiGate CloudFormation script and have it running the same way it has run successfully dozens of times in the past. We no longer have to spend time troubleshooting issues. It makes life much easier."

– *Nikolay Chigrin, Senior System Engineer, AWS, S2 Global*

Details

Customer: S2 Global

Industry: Technology

Location: Hawthorne, California

Business Impact

- Reduced time to deploy a firewall in AWS by 80%
- Improved efficiency throughout the IT security team
- Enabled S2 Global to stay ahead of the curve on security issues
- Minimized one-off human errors because all deployments are identical

"We wanted to simplify the settings and have the same environment mirrored, whether on premises or in the cloud," Chigrin says. "Then, if our engineers needed to upgrade something or change configurations down the road, they would always have the same path for connecting to every firewall, and for finding all the appropriate pieces of hardware and software to target."

From there, Chigrin looked for a way to automate his portion of the NGFW deployment. "When I create the full stack for a client's AWS environment, I need to spin up the FortiGate VM and enable NAT [network address translation]," he says. "I upload a temporary FortiGate license that I received from Fortinet and initiate the network and subnets behind the firewall and NAT. I have to name those, attach the internet gateways, etc. Once I get all that set up, the system moves on to our security engineer for additional configuration." This process previously took Chigrin three to four hours per NGFW.

"I wanted to speed that up," he adds. "Since we standardized the firewall's fundamental configuration, my portion of the deployments are all carbon copies. I decided to test a rollout through AWS CloudFormation." Because Fortinet is an AWS CloudFormation third-party resource provider, security teams can use CloudFormation to provision and manage Fortinet resources in the same way they would manage AWS resources. Thus, Chigrin wrote a CloudFormation script to create a VM, enable NAT, then run the basic steps of initialization that he is responsible for. "I put everything in the CloudFormation script. Now it takes just a couple of minutes to spin up a new firewall and 40 minutes for entire stack deployment."

Solution

- FortiGate VM for AWS

"CloudFormation has reduced the amount of time to deploy an entire infrastructure by about 80%, including deploying and preconfiguring the firewall. Compared with other firewalls I have used, with Fortinet CloudFormation resource providers, FortiGate solutions are super simple to operate and set up."

– *Nikolay Chigrin, Senior System Engineer, AWS, S2 Global*

Automation Makes Life Easier for IT Staff

The CloudFormation script has substantially increased efficiency for Chigrin and his colleagues. "CloudFormation has reduced the amount of time to deploy an entire infrastructure by about 80%," he says. "I had never used Fortinet solutions before I started with S2 Global. It was pretty easy for me to go through the interface, check the settings, and verify the IP addresses and networks. Compared with other firewalls I have used, with Fortinet CloudFormation resource providers, FortiGate solutions are super simple to operate and set up."

Chigrin is confident that the solution is providing adequate security to meet clients' needs and his company's internal security policy. "Our relationship with Fortinet enables us to stay a step ahead," he says. "The news published by Fortinet—the upgrade announcements and other bulletins—are really informative. They give us the full picture of what we have to do to keep our clients' data and applications secure, as well as how fast it can be done."

Clients do not often comment on S2 Global's security systems, which Chigrin takes to mean they are satisfied. "No news is good news; if they had security concerns, we would hear about it," he says. "As an example, when new encryption protocols are announced and we need to update our firewalls, we work with Fortinet to get that done. Then, when our clients start asking, 'Guys, are you going to use the new encryption protocols?' we can say, 'We have already been using them for three weeks.'"

Finally, Chigrin sees automation as a means of reducing the risk of human error. He describes a situation that happened shortly after he started with S2 Global: He was redeploying a FortiGate VM NGFW and did not realize that he needed to disable the source destination check. He and a colleague spent a couple of hours trying to figure out why the system was not pinging from inside. They eventually figured out the problem and were able to solve it quickly.

By contrast, however, "with our new automated setup, we just upload the FortiGate CloudFormation script and have it running the same way it has run successfully dozens of times in the past," Chigrin says. "We no longer have to spend time troubleshooting these kinds of issues. It makes life much easier. Standardization is my last name."

FORTINET

www.fortinet.com

October 10, 2020 12:58 AM

792924-0-0-EN

D:\Fortinet\Case Study\Blue Case Study\S2 Global\cs-FA-automating-fortinet-solution-rollouts-in-aws-1022020