SOLUTION BRIEF

Fortinet and HashiCorp Integrated Solution

Simplify Security Operation Across Multi-cloud Environments Through Event-driven Automation

Executive Summary

As organizations embark on their journey to accelerate the application lifecycle residing on their private data centers, public clouds, and across physical and virtual form factors, there is an increasing need to automate all related security operations. To support these efforts, Fortinet offers official HashiCorp Terraform and Consul-Terraform-Sync provider modules for FortiOS and FortiManager, which enable multiple new network infrastructure automation opportunities for customers.

Challenges

Over 90% of enterprises are distributing their workloads across multi- and hybrid clouds. As a result, cloud and network operational teams are overwhelmed managing infrastructure and deployments across their various different cloud environments. Organizations are experiencing challenges connecting applications and data across clouds, data centers, and branches, often at the expense of stringent security practices and operational efficiency. Increasing the likelihood of the number-one security risk affecting cloud deployments: human-driven misconfigurations.

With organizations leveraging hybrid cloud and multi-cloud to increase agility, they are looking to automate and scale their DevOps lifecycle through the use of Infrastructure-as-Code (IaC) to provision, configure, and tear down needed cloud infrastructure on demand.

Joint Solution Components

- Fortinet FortiOS
- Fortinet FortiManager
- HashiCorp Terraform
- HashiCorp Consul-Terraform-Sync

Joint Solution Benefits

- Automated and simplified network infrastructure deployment and management
- Automated Day-2 service creation and update
- Scalability
- Compliance

FORTINET FABRIC-READY

Joint Solution

HashiCorp and Fortinet have come together to provide a joint solution with FortiManager using HashiCorp's Network Infrastructure Automation (NIA) tool, HashiCorp Consul-Terraform-Sync (CTS). Leveraging the integration, organizations can deploy infrastructure and operate it like software code without compromising on security or compliance. The deployment and operation of security can be tied directly to infrastructure automation, enabling organizations with business agility and transition to a highly automated, self-service model employing a DevOps mindset.

Fortinet's CTS support enables IT teams to transition security into a DevSecOps operating model and insert themselves into the CI/CD continuum. Security teams can quickly deploy Day-0 configurations or make iterative changes for Day-1 and Day-2 operations to provision, deploy, and manage resources, such as devices, IP addresses, DNS, Internet Protocol security (IPsec), trust/untrust zones, firewall policies, and more. Changes can be pushed into a repository that are subsequently picked up by a CI/CD system that seamlessly updates the production environment.

Joint Solution Integration

Fortinet and HashiCorp have come together in Fortinet's open ecosystem to deliver robust and deep security automation for DevOps-driven multi-cloud and hybrid-cloud deployments leveraging the Fortinet Security Fabric. Fortinet offers the broadest cloud-native security with tight integrations on major cloud platforms like Azure, Google Cloud, and AWS, further enabling customers to automate, orchestrate, and simplify their operations securely between all major public cloud platforms, network edges, and data centers with Terraform integration.

The Fortinet Security Fabric is coordinated through the FortiManager management center, which provides NetOps, SecOps, and DevOps teams with a single-pane-of-glass interface to simplify security orchestration, enforcement, and compliance. Additionally, the FortiGate virtual next-generation firewall can be deployed natively in multiple private and public cloud environments. This provides robust, scalable network security across the distributed network—enabling secure access to cloud-based applications and resources, establishing and maintaining virtual network protection in any cloud, and ensuring consistent and robust network security policies across a multi-cloud environment.

FortiManager Terraform Provider

Terraform is an open-source IaC software tool that provides a consistent CLI workflow to manage hundreds of cloud services. Terraform codifies cloud APIs into declarative configuration files.

At a high level, Terraform functions as an abstraction layer by providing a uniform language for invoking CRUD (create, read, update, delete) operations on various systems. However, to perform those functions in different environments, Terraform requires a layer responsible for translating between the Terraform configuration language and the specific product operations invoked via API. This layer is called the Terraform provider.

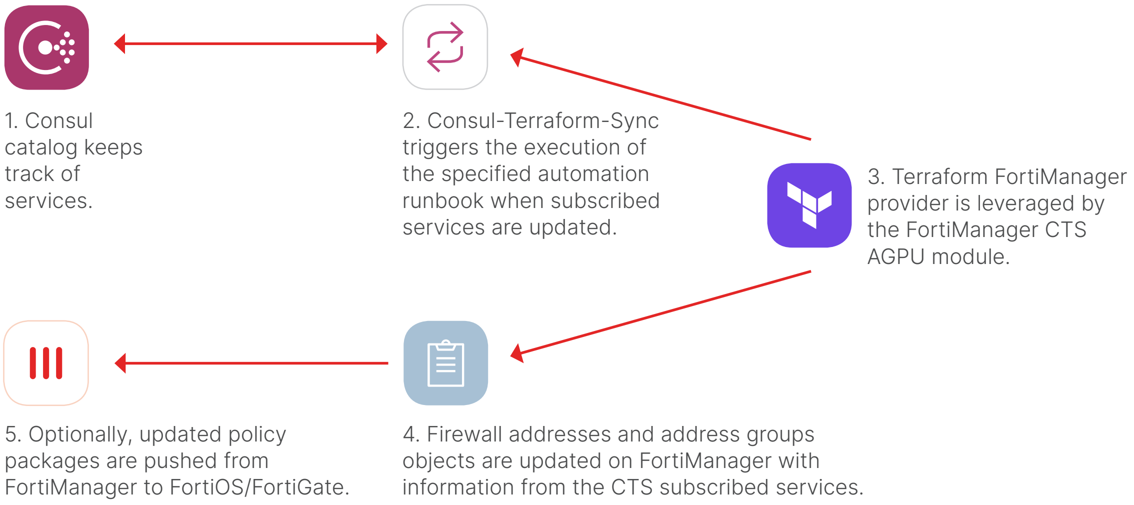
The Terraform provider enables security teams to use a declarative syntax to deploy security IaC in a fashion similar to the strategies used by application developers. Terraform can use code to orchestrate various cloud objects, devices on the cloud, and orchestrate the objects in these devices, which greatly improves the flexibility of deployment, shortens the deployment cycle, and makes large-scale dynamic deployment a reality, of great significance for deploying FortiOS on the cloud.

The Fortinet Terraform provider uses Terraform to automate infrastructure and security deployments, enabling an agile operating model based on Terraform providers for FortiOS and FortiManager. This solution can be used to deploy anything from a single VPC or VNet to complex multi-cloud environments and solutions for on-premises environments. The Fortinet Terraform provider also works with Terraform Enterprise, enabling organizations to effectively collaborate and use it in conjunction with other Terraform providers.

FortiManager Consul Provider: The Consul-Terraform-Sync Module

Consul uses service identities and traditional networking practices to help organizations securely connect applications running in any environment. The Consul-Terraform-Sync runs as a daemon that enables a publisher-subscriber paradigm between Consul and FortiManager-based devices to support network infrastructure automation (NIA).

As shown in Figure 1, Consul-Terraform-Sync subscribes to updates from the Consul catalog and executes one or more automation "tasks" with appropriate value of service variables based on those updates. Consul-Terraform-Sync leverages Terraform as the underlying automation tool and utilizes the Terraform provider ecosystem to drive relevant change to the network infrastructure. Each task consists of a runbook automation written as a compatible Terraform module using resources and data sources for the underlying network infrastructure provider.



1. Consul catalog keeps track of services.

2. Consul-Terraform-Sync triggers the execution of the specified automation runbook when subscribed services are updated.

3. Terraform FortiManager provider is leveraged by the FortiManager CTS AGPU module.

4. Firewall addresses and address groups objects are updated on FortiManager with information from the CTS subscribed services.

5. Optionally, updated policy packages are pushed from FortiManager to FortiOS/FortiGate.

Figure 1: The FortiManager Terraform and CTS-AGPU module.

Joint Use Cases

1. **Bootstrapping firewall configurations** – In larger organizations, where FortiGate firewalls are frequently deployed to support different applications, Terraform enables the ability to create a baseline configuration that can be provisioned as soon as an organizational unit requests firewall functionality. This not only helps accelerate the time to securely deploy an application, but also eliminates configuration errors.
2. **Large-scale change management** – Any FortiGate assets automatically provisioned using Terraform templates can be automatically added to an inventory management system. This ensures that when a configuration update needs to take place across multiple assets, those updates are automatically rolled out across all assets, thereby eliminating the chance of creating a security gap caused by a failure to update all devices.
3. **Integrating firewall lifecycle management elements into customer applications** – In more specific cases, where changes are being made to applications that are already protected by FortiGate firewalls, organizations can integrate FortiGate change management routines, such as including security policy updates as part of application change routines.
4. **Controlling multi-cloud application security** – FortiGate solutions on various platforms can now benefit from the Terraform abstraction layer by configuring similar functionality on FortiGate solutions regardless of the cloud platforms they are deployed on. This allows customers to focus on functionality rather than configuration and helps to achieve consistent security and implement streamlined change management practices to ensure security is always up-to-date across their multi-cloud environment.
5. **Automatic network updates** – Network infrastructure is updated automatically based on changes in the HashiCorp Consul catalog leveraging the Terraform CLI on the local node. This includes core networking use cases for practitioners, including applying firewall policies, updating load balancer member pools, and more.
6. **Dynamic lifecycle managament** – Day-2 application networking delivery lifecycle is managed more dynamically while providing governance and security oversight of infrastructure using Terraform as the automation engine.

About HashiCorp

HashiCorp is a leader in multi-cloud infrastructure automation software. The HashiCorp software suite enables organizations to adopt consistent workflows and a standardized approach to automating the critical process involved in delivering applications in the cloud: infrastructure provisioning, security, networking, and application deployment.

May 18, 2022 2:27 AM
1609862-0-0-EN