SOLUTION BRIEF

Fortinet and Red Hat Security Solution

Efficiently scale and automate security for hybrid and multi-cloud environments with machine learning and centralized management

Executive Summary

The Fortinet–Red Hat partnership enables innovative and high-performance security solutions that can be easily managed and scaled with automation to reduce complexity. Integrations between multiple Fortinet and Red Hat solutions provide options to secure applications, workloads, networks, and clouds that can adapt to evolving business needs.

Challenge

The attack surface continues to expand and infrastructures are more distributed than ever, encompassing multi-cloud, on-premises environments, and edge networks. Combined with today's rapid pace of application development and the risk of misconfigurations and vulnerabilities, managing security has become more complex for understaffed teams.

Red Hat and Fortinet have built a partnership to automate the deployment and management of security tools across the entire environment. By integrating Red Hat and Fortinet solutions, customers can efficiently scale and manage security with easy-to-use playbooks and orchestration.

Joint Solution Description

With Red Hat and Fortinet, security is made more efficient through automation. Provision, update, and take action quickly with easy-to-use Red Hat playbooks and centralized management with Fortinet. The seamless integration enables automated configuration changes and detection and remediation of security issues with comprehensive, end-to-end visibility.

Red Hat Ansible provides automation and orchestration for Fortinet security solutions, including FortiGate, FortiSwitch, FortiManager, FortiAnalyzer, FortiWeb, and FortiADC, with over 639 modules for FortiOS and over 896 modules for FortiManager. These modules comprise an extensive library of actions for use in Ansible playbooks, making it easy to create, manage, and update infrastructure ranging from physical devices, virtual machines, containers, and more. The vast library of modules developed and maintained by Fortinet provide more automation options than competitors can offer.

Red Hat OpenStack makes provisioning new FortiGate virtual appliances simple. OpenStack-based clouds provide the environment needed for elastic, on-demand multitenant applications. Customers can deploy a mix of FortiGate hardware and virtual appliances for scalable coverage managed from a common centralized management platform.

Solution Components

- Red Hat Ansible, OpenShift, and OpenStack
- Fortinet FortiCNP cloud-native protection, FortiGate, FortiSwitch, FortiManager, FortiAnalyzer, FortiWeb, and FortiADC

Solution Benefits

- Secure applications, multi-cloud and hybrid environments
- Reduce risk and complexity across distributed infrastructure
- Automate deployments and management with playbooks
- Scale efficiently and increase productivity

FORTINET FABRIC-READY

To secure cloud workloads and applications, Fortinet FortiCNP cloud-native protection and FortiWeb can be used with Red Hat OpenShift to integrate security into the continuous integration/continuous deployment (CI/CD) life cycle. Customers benefit from protection against known and unknown threats and misconfigurations, automated policy enforcement for response actions, and overall compliance with security best practices using industry-leading benchmark baselines.

Joint Solution Integration

Scale and Automate Security with Red Hat Ansible, FortiManager, and FortiOS

Use Case

Red Hat Ansible allows developers to set up automation to provision, deploy, and manage compute infrastructure across cloud, virtual, and physical environments. With Red Hat Ansible playbooks, security, network, and DevOps teams can easily deploy and manage machines, switches, and containers with automation.

When used in combination with Fortinet's operating system, FortiOS, automation can be applied to a simplified policy and management framework that consolidates multiple technologies into the Fortinet Security Fabric.

Ansible playbooks can also be used with:

- **FortiManager** for automation-driven centralized management of Fortinet devices, such as FortiGate Next-Generation Firewalls (NGFWs) and Secure SD-WAN, from a single console
- **FortiAnalyzer** for centralized logging and reporting of Fortinet Security Fabric solutions
- **FortiSwitch** for LAN connectivity and Secure SD-Branch deployments
- **FortiWeb** for deploying protection for web applications and APIs
- **FortiADC** for deploying application availability, application security, and application optimization

Modules built and maintained by Fortinet execute specific functions and API calls in Fortinet products within playbooks. These extensive integrations enable management of Fortinet Security Fabric solutions, DevOps deployments, configuration changes, detection and remediation of security incidents.

The integration of Fortinet security solutions with Red Hat Ansible allows organizations to efficiently scale security. If an organization needs to increase their number of firewalls, it can be a big project to deploy new hardware and keep all devices up to date without disrupting business services. With FortiGate NGFWs and FortiManager for centralized management, the deployment and update processes can be automated using Ansible playbooks.

How It Works

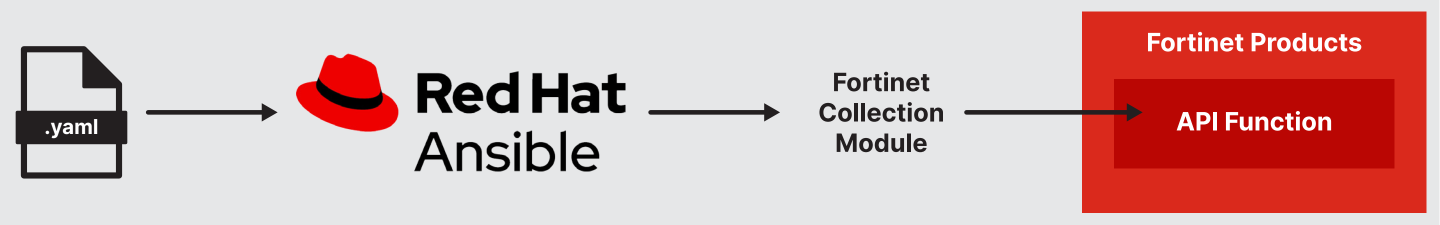


Figure 1: A YAML human-friendly configuration file, or playbook, creates an automation request to Red Hat Ansible, which uses a Fortinet module to affect change via an API call.

Ansible playbooks use a YAML file to describe automation jobs in a human-readable format. It doesn't require agents or additional customized security infrastructure. Ansible uses modules to understand interactions with Fortinet products and to display those resources to Ansible. Fortinet has developed both specific and generic modules. The specific function modules execute a single known function on a target device, such as a call to a specific API to change a route. Generic function modules are used to execute any API call on the target system.

Over 639 modules are available for FortiOS, covering all CMDB API features. Over 896 modules are available for FortiManager, along with a generic module to address features that do not yet have specific function modules or use dynamically named APIs. Custom modules can be added from Ansible Galaxy in the form of collections. The Fortinet modules for use with FortiOS, FortiSwitch, FortiManager, FortiAnalyzer, FortiWeb, and FortiADC are available from both Ansible Galaxy and GitHub.

Deploy Virtual Network Security On-Demand with Red Hat OpenStack and FortiGate Virtual Appliances

Use Case

The FortiGate NGFW is a high-performance network security virtual appliance that adds intrusion prevention, application and user visibility, SSL inspection, and unknown threat detection to the traditional firewall. Red Hat OpenStack Platform is a cloud computing platform that virtualizes resources from industry-standard hardware, organizes those resources into clouds, and manages them so users can access what they need—when they need it. When the FortiGate virtual appliance is used with Red Hat OpenStack Platform, the fully containerized virtual machine can be quickly deployed and managed in a scalable private cloud to increase defenses.

Running OpenStack services in containers lets you manage and scale each service independently. This simplifies deployment, upgrades, rollback, and management to deliver increased control and flexibility. The FortiGate virtual appliance image is validated by Fortinet to ensure top functionality.

How It Works

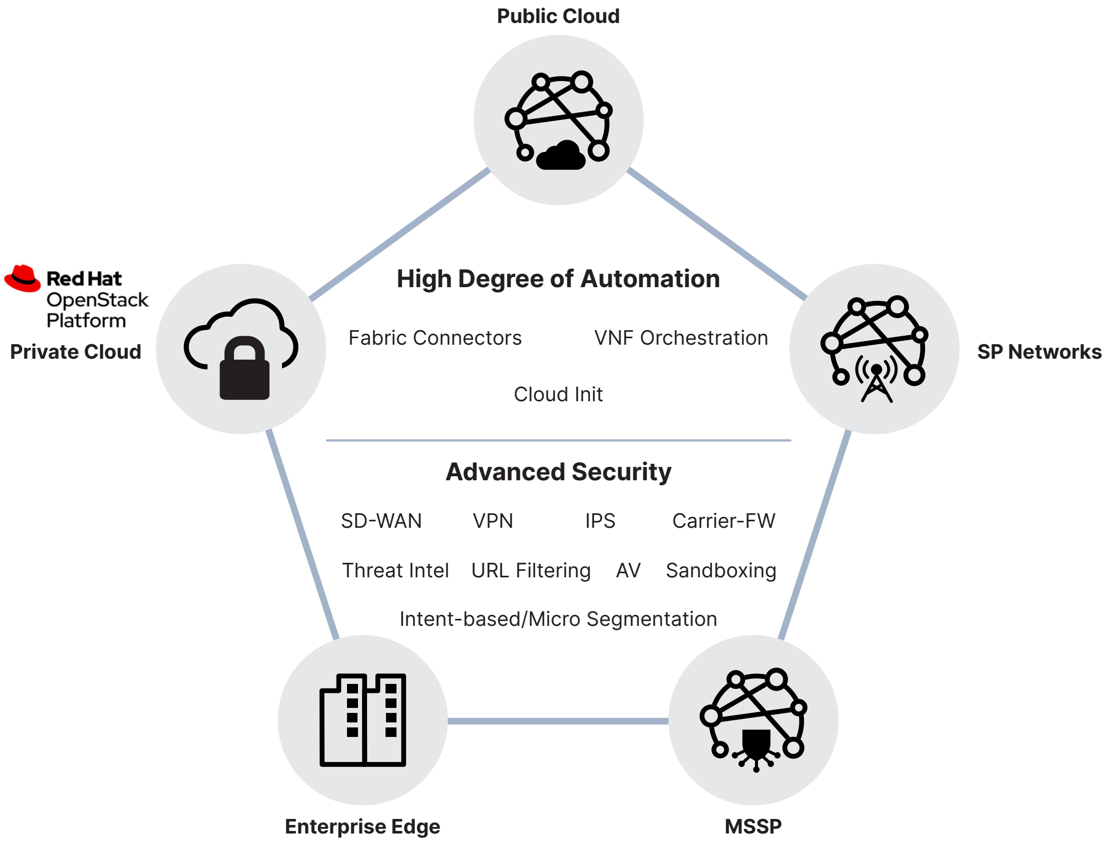
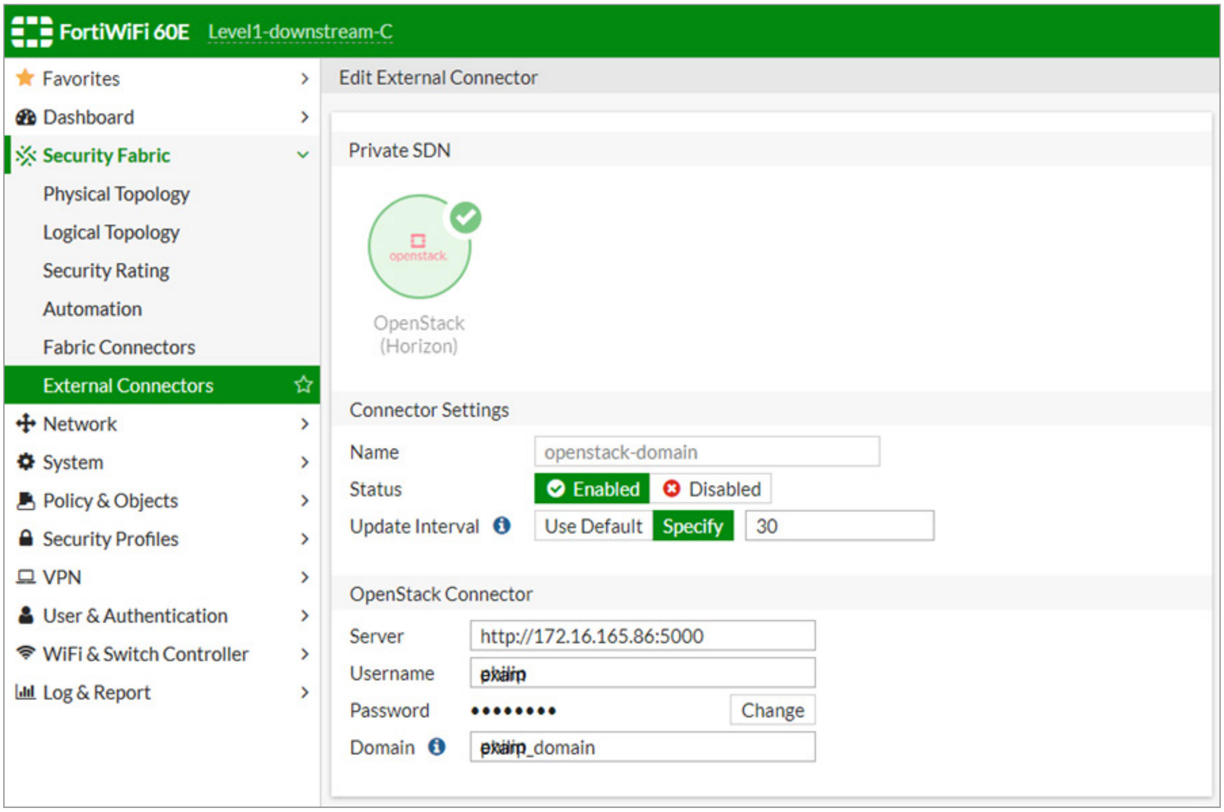


Figure 2: Get advanced security and automation when deploying FortiGate VM with the Red Hat OpenStack Platform.

FortiGate VM can be deployed as a VNF on Red Hat OpenStack and its deployment can be automated directly using Cloud-Init or Heat Templates. Once the FortiGate VM is fully deployed, the OpenStack Connector can be used to retrieve Workload dynamic IP address information, which can then be used on the security policies.



Edit External Connector

Private SDN

Connector Settings

Name: openstack-domain

Status: ● Enabled ○ Disabled

Update Interval: Use Default **Specify** 30

OpenStack Connector

Server: http://172.16.165.86:5000

Username: exam

Password: ••••••••

Domain: exam_domain

Workload acceleration techniques such as SR-IOV and DPDK are fully supported by FortiOS and can be leveraged when deploying FortiGate VM on Red Hat OpenStack to boost performance. By using NSH Chaining, FortiGate VM can be deployed for Service Insertion/Chaining function for networks that require zero trust.

Develop and Deploy Secure Applications and Workloads with Red Hat OpenShift, Fortinet FortiWeb, and FortiCNP Cloud-Native Protection

Use Case

Red Hat OpenShift is the Kubernetes platform that allows DevOps teams to build, manage, and deploy cloud-native products across hybrid and multi-cloud environments by providing a trusted foundation. Fortinet FortiWeb is a web application firewall (WAF) that protects hosted web applications from attacks that target known and unknown exploits. With machine learning (ML) and AI, FortiWeb provides protection for web applications and APIs built or deployed on Red Hat OpenShift environments.

Using ML to model each application, FortiWeb defends applications from known vulnerabilities and zero-day threats, including OWASP Top 10 web vulnerabilities. FortiWeb can be integrated into the microservices architecture for use as a cloud-native, DevOps-enabled, and containerized WAF.

FortiCNP cloud-native protection integrates security into containers to protect cloud workloads in Red Hat OpenShift environments. It detects vulnerabilities and non-compliant Kubernetes clusters, and it continuously monitors and scans registries to provide ongoing protection.

How It Works

Both FortiWeb and FortiCNP can be integrated into the CI/CD pipeline to help DevOps teams deliver secure applications and deploy to container registries with Red Hat OpenShift. When FortiWeb and FortiCNP are combined with FortiGate VM for ingress-egress cloud security, they form the only integrated cloud security solution addressing network security, web application security, and cloud platform security in a comprehensive and tightly integrated solution.

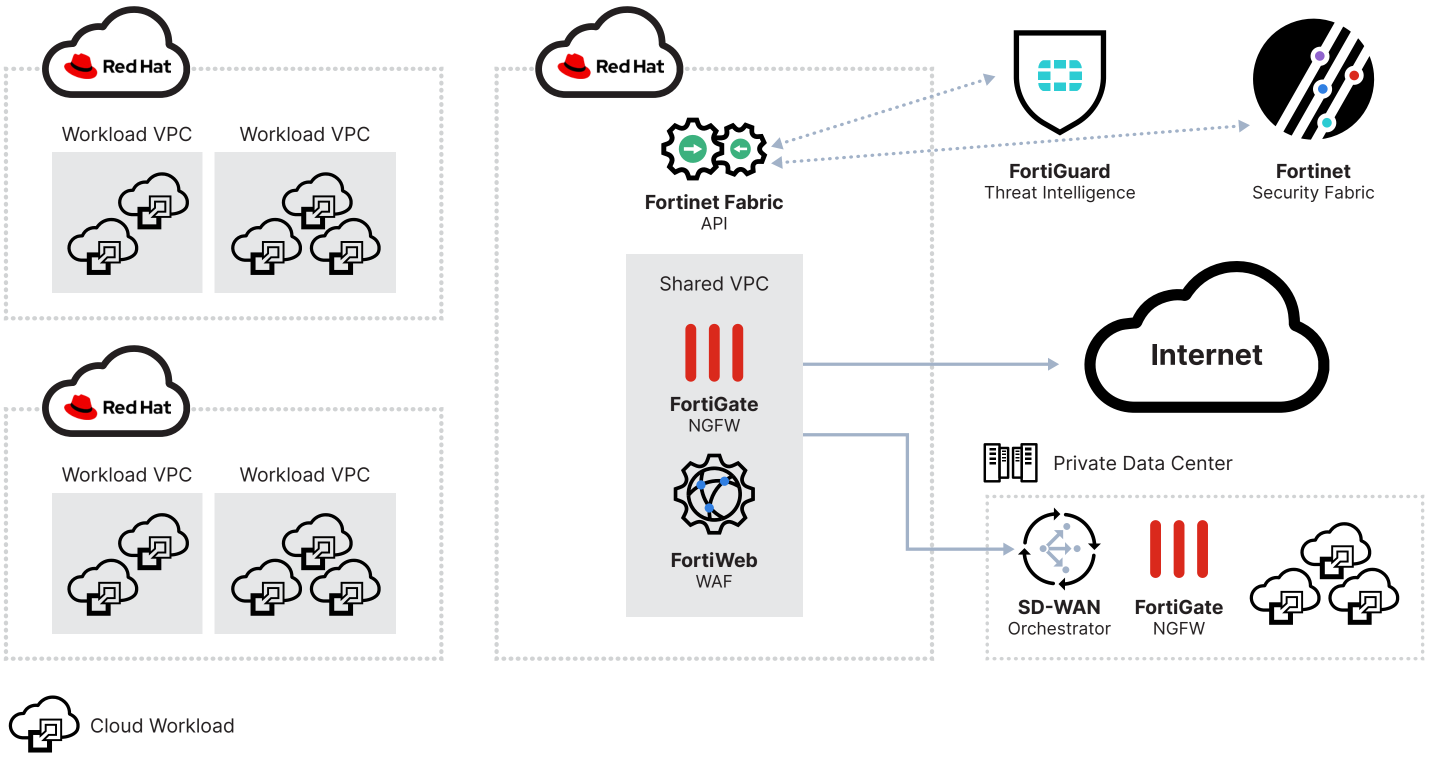


Figure 3: Develop, manage, and deploy secure cloud-based applications, APIs, and workloads with Red Hat OpenShift and Fortinet.

About Red Hat

Red Hat is the world's leading provider of enterprise open-source software solutions, using a community-powered approach to deliver reliable and high-performing Linux, hybrid cloud, container, and Kubernetes technologies. Red Hat helps customers integrate new and existing IT applications, develop cloud-native applications, standardize on our industry-leading operating system, and automate, secure, and manage complex environments. Award-winning support, training, and consulting services make Red Hat a trusted adviser to the Fortune 500. As a strategic partner to cloud providers, system integrators, application vendors, customers, and open source communities, Red Hat can help organizations prepare for the digital future.

October 4, 2022 1:52 AM
1786903-0-0-EN