Cisco Secure Firewall Cloud Native

Contents

The need for on-demand, scalable, and agile security services has grown tremendously with the "work from anywhere" culture and with the need for employees to access corporate applications from their personal devices. Organizations typically build scalable systems by acquiring individual components and then manually automating and orchestrating them with tools from different vendors. This approach creates complexity, making provisioning, management, and troubleshooting of scalable services difficult.

Cisco® Secure Firewall Cloud Native provides a platform for deploying scalable and resilient security services using Kubernetes orchestration. It alleviates complexities associated with scalability, load balancing, and service availability. This allows SecOps teams to focus exclusively on security posture management and enforcement.

With Secure Firewall Cloud Native, you have flexibility to choose the performance you need for your organization. It offers agile and elastic security in public and private clouds. Its scalable and feature-rich VPN capability provides secure remote access for employees, partners, and suppliers and protects your workloads against increasingly complex threats with industry-leading security controls.

Product overview

Secure Firewall Cloud Native provides a common framework to simplify management of security services and a platform that automatically scales and controls them. Customers can choose which services they want to provision, empowering teams with the ability to deploy and scale security based on need.

It uses Kubernetes to provide scalability and resiliency. Customers only need to configure the overall security service. Behind the scenes, Secure Firewall Cloud Native monitors the health and performance of each service, scaling up or down based on user-defined metrics. It customizes configurations for each instance of the service running at any given time, forwarding events and logs to user-configured sinks. Additionally, it offers automatic failure recovery capabilities.

Security policies are managed by Cisco Defense Orchestrator (CDO), a feature-rich software-as-a-service (SaaS) management application with a simple GUI, or using REST APIs. Secure Firewall Cloud Native provides extensive automation capabilities, including options to deploy it as infrastructure as code (IaC).

Secure Firewall Cloud Native is available on Amazon Web Services at release and will roll out on additional platforms soon.

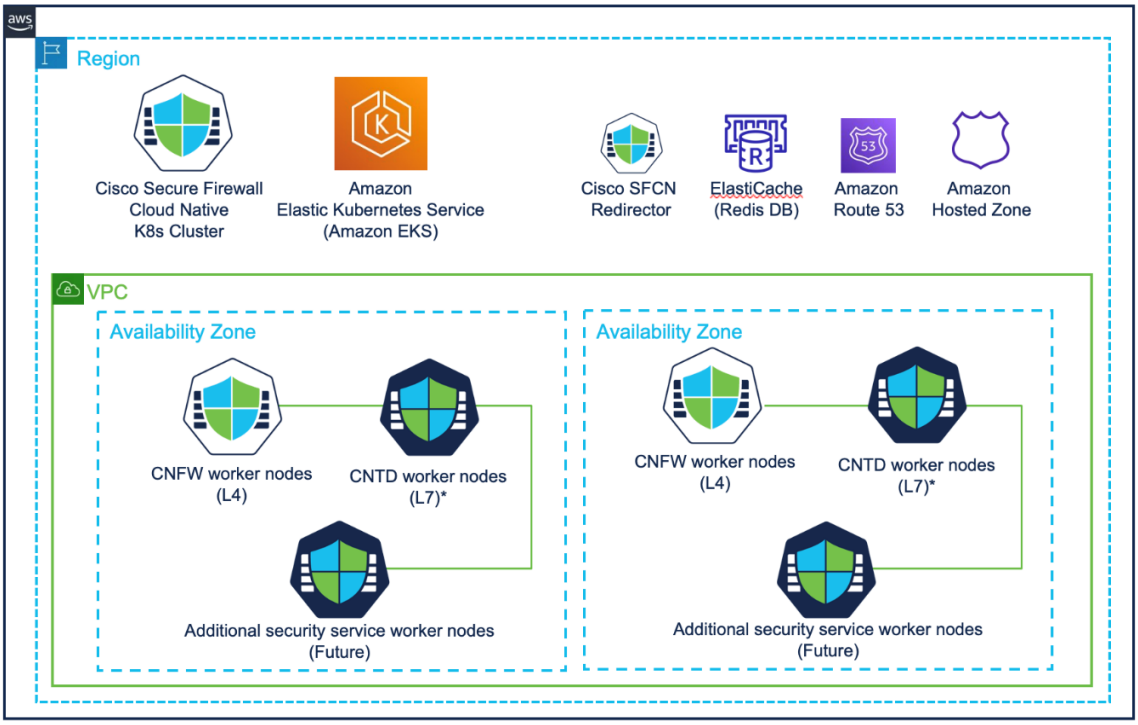

Figure 1.
Cisco Secure Firewall Cloud Native overview

Scalable VPN service using Secure Firewall Cloud Native

To deploy a scalable VPN service, customers deploy Secure Firewall Cloud Native with the included Cloud Native Firewall (CNFW) service.

The three main components that are deployed as part of the CNFW service include:

1. **Control plane pods:** Control plane pods are responsible for configuration of the VPN service. They accept configuration from management applications or from REST APIs. These pods also validate and distribute the configuration to the Enforcement Points.
2. **Enforcement point pods:** Enforcement point pods are responsible for the actual termination of VPN sessions and forwarding of traffic.
3. **Redirector pods:** Redirector pods are responsible for smart load balancing of sessions across enforcement point pods based on real-time assessment of load on each enforcement point pod.

All components are automatically deployed when you install Secure Firewall Cloud Native. It is recommended that customers base their sizing decisions on the number of enforcement point pods they need deployed in the platform. This recommendation is based on expected peak VPN throughput and average VPN throughput. Do not be concerned if your initial estimates are not accurate, as the system is designed for high scalability and elasticity and estimates can always be adjusted with ease.

Resource utilization details for AWS

Each component is optimized to run on a specific type of instance on AWS. The table below lists the instance type details for each component.

Component	Instance type
Control plane pod	m5.xlarge
Enforcement point pod	m5.xlarge
Redirector pod[1]	m5.xlarge

[1] Redirector functionalities need a Redis database, and that will be installed on an m5. large instance by default. The default can be easily changed to use larger or smaller instance types to allocate more (or less) memory.

The installer takes care of deploying each component on the right instance type.

Performance metrics

VPN performance of Secure Firewall Cloud Native is equal to the sum of performance of each enforcement point pod. The system is highly elastic and adds or deletes enforcement point pods dynamically based on current performance requirements. The table below lists tested VPN performance of each enforcement point pod.

Feature	Performance
IPsec VPN throughput (AES 450B UDP test)[1]	1.5 Gbps
IPsec VPN peers	2000
Cisco AnyConnect® or clientless VPN user sessions	2000

[1] The VPN throughput and the number of sessions depend on the configuration and VPN traffic patterns. These elements should be taken into consideration as part of your capacity planning.

Based on performance per pod, one can set limits of scaling:

1. Minimum number of enforcement point pods: this is the number of pods that are always provisioned.
2. Maximum number of enforcement point pods: this is the maximum number of pods that can be provisioned at any point in time.

Secure Firewall Cloud Native monitors the load using specified VPN parameters and makes decisions dynamically to scale the number of pods within the specified range based on load.

Scalability of components

The table below shows the tested scalability limits of each component.

Attribute	Scale
Maximum number of enforcement pods that can be deployed in one instance of Secure Firewall Cloud Native	75*
Maximum number of enforcement pods that can be managed by one control plane pod	75*

* These numbers are tested and validated through Cisco. Talk to your Cisco sales representative if you require greater scale than what has been tested.

Licensing for Secure Firewall Cloud Native

Services that run on Secure Firewall Cloud Native are licensed. Each service is licensed using Cisco Smart Licensing, based on the number of CPU cores assigned to the service.

For the CNFW service, customers must have four licenses available in their Cisco Smart Licensing Account for each enforcement point pod that is deployed.

Smart Software Licensing

Cisco Smart Software Licensing makes it easier to buy, deploy, track, and renew Cisco licenses. You will enjoy:

- Simplified purchase and activation of the virtual appliance.
- Easier license management and reporting of virtual appliances due to license pooling.
- Automatic license activation when the virtual appliance is provisioned.

Customers, select partners, and Cisco can view product entitlements and services in the Cisco Smart Software Manager. Configuration and activation are done with a single token. Secure Firewall Cloud Native will self-register with a Cisco server in the cloud, eliminating the need to register products with Product Activation Keys (PAKs). Instead of using PAKs or license files, Smart Software Licensing establishes a pool of software licenses or entitlements that can be used across your business. When a CNFW enforcement point pod is instantiated on a customer's premises, an entitlement for each CPU core is subtracted from the pool. When a licensed CNFW enforcement point pod is decommissioned, or when it is de-instantiated within the Smart Software Manager, its entitlement is added back to your pool.

With the Smart Software Manager, you can manage license deployments throughout your organization easily and quickly. You can also manage multiple products from Cisco that support Smart Software Licensing.

Cisco Secure Firewall Cloud Native uses Smart Software Licensing exclusively.

Cisco environmental sustainability

Information about Cisco's environmental sustainability policies and initiatives for our products, solutions, operations, and extended operations or supply chain is provided in the "Environment Sustainability" section of Cisco's Corporate Social Responsibility (CSR) Report.

Reference links to information about key environmental sustainability topics (mentioned in the "Environment Sustainability" section of the CSR Report) are provided in the following table:

Sustainability topic	Reference
Information on product material content laws and regulations	Materials
Information on electronic waste laws and regulations, including products, batteries, and packaging	WEEE compliance

Cisco makes the packaging data available for informational purposes only. It may not reflect the most current legal developments, and Cisco does not represent, warrant, or guarantee that it is complete, accurate, or up to date. This information is subject to change without notice.

Cisco Capital

Flexible payment solutions to help you achieve your objectives

Cisco Capital makes it easier to get the right technology to achieve your objectives, enable business transformation and help you stay competitive. We can help you reduce the total cost of ownership, conserve capital, and accelerate growth. In more than 100 countries, our flexible payment solutions can help you acquire hardware, software, services and complementary third-party equipment in easy, predictable payments. Learn more.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **https://www.cisco.com/go/offices**.

Printed in USA C78-744973-00 06/21