SOLUTION BRIEF

Fortinet and Cactus eSecurity Security Solution

Firewall Orchestration and Rules Management

Executive Summary

Fortinet and Cactus eSecurity unite to present a firewall orchestration and rules management solution. Fortinet and Cactus eSecurity offer an approach to report on Fortinet device rulebases and regularly certify rules to clean up an organization's configurations and comply with regulatory requirements.

Financial institutions and other sectors must comply with regulatory requirements. Active firewall rules require at least a once-a-year certification cycle. Clean up your unused firewall rules, which might comprise more than 50% of your rules base.

Joint Solution

Solution Components

The Cactus eSecurity Firewall Orchestrator offers network security policy management, enabling the creation of reports on the current firewall configuration or changes in the last few days. It also offers automation by reading firewall configurations via REST API and getting access to configuration data via the FortiManager and FortiOS Firewall Orchestrator GraphQL API. It also provides out-of-the-box recertification of your firewall rules, enabling you to keep track of your rules and, at the same time, meet regulatory requirements.

Fortinet FortiGate Next-Generation Firewalls (NGFWs) provide industry-leading threat protection and decryption at scale with a custom ASIC architecture. They deliver secure networking with integrated features such as SD-WAN, switching and wireless, and 5G. Converge your security and networking point solutions into a simple-to-use, centralized management console powered by a single operating system, FortiOS, and simplify IT management.

Fortinet FortiManager delivers unified management for consistent security across complex hybrid environments, protecting against security threats. Key benefits include accelerated zero-touch provisioning with best-practice templates for deployment at the scale of SD-WAN and streamlined workflows within the Fortinet Security Fabric.

Integration

The Firewall Orchestrator integration enables management of rules for the FortiGate NGFW directly or via the FortiManager. This allows users to report on Fortinet device rules bases and certify controls regularly to clean up configurations and comply with regulatory requirements.

Solution Components

- Fortinet FortiGate and FortiManager
- Cactus eSecurity Firewall Orchestrator (Import Module, Reporting module, Workflow module for firewall change requests, Recertification module, Compliance module)

Solution Benefits

- Recertify your firewall rules regularly to remove unwanted rules to comply with regulatory requirements for financial institutions and other industry sectors.
- Get an overview of your existing configuration via different reports (unused rules, changes, current rules).
- Enhance your firewall rule life cycle by using the built-in workflow module for requesting, approving, planning, automating, and implementing configuration changes.

FORTINET FABRIC-READY

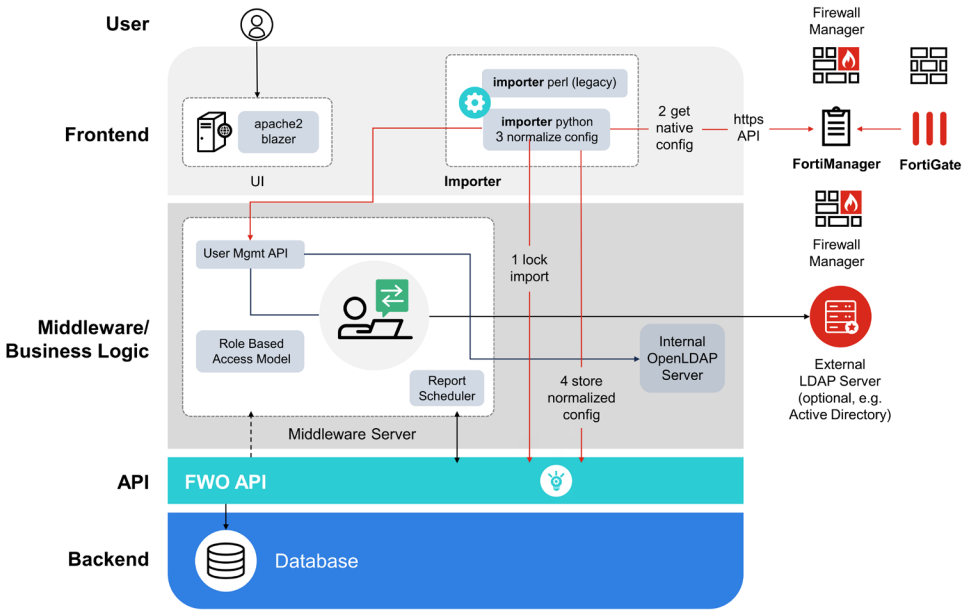

Figure 1: The Fortinet and Cactus eSecurity integration architecture

Joint Use Cases

Use Case #1: Manage and Optimize Your Rulebase with the Cactus eSecurity Firewall Orchestrator Recertification Module
Firewall Orchestrator allows you to configure an individual scheme defining who should review which firewall rules how often in order to recertify them. The goal is to keep your firewall configuration as close to the least privilege state as possible by removing all of the rules that are not needed.

This can be done by dynamically assigning firewall rules to application owners based on the IP addresses used within the rule's source or destination.

The resulting firewall orchestrator process then ensures a regular distributed and scalable review of all firewall rules.

Use Case #2: Set Up a Partly Automated Process for Requesting and Implementing Firewall Changes
Firewall Orchestrator comes with a built-in customizable workflows that allow you to define roles for users who are able to request firewall rules. You can also set up an approver group and define a group of people who can implement the requests.

The process is fully documented within firewall orchestrator, allowing you to satisfy audit requirements. Additionally, you may use the firewall orchestrator API to integrate with existing workflow tools such as ServiceNow to use them as a front end, accessing the firewall data via the firewall orchestrator API.

About Cactus Security

Cactus eSecurity brings a balance of technology orientation and conceptual simplicity into projects. In this way, we can offer both cutting-edge technology and down-to-earth best practice tips gathered in helping enterprise customers with their network security during the last 20 years. Our main focus is firewall orchestration, i.e. helping to simplify and automate enterprise network security. Apart from firewalling, Cactus eSecurity also supports customers in planning, implementing and operating other network security controls like virtual private networks, intrusion prevention systems, anomaly detection and many others.

March 1, 2024 10:15 PM
2340882-0-0-EN