SOLUTION BRIEF

FortiCare Firewall Migration Services

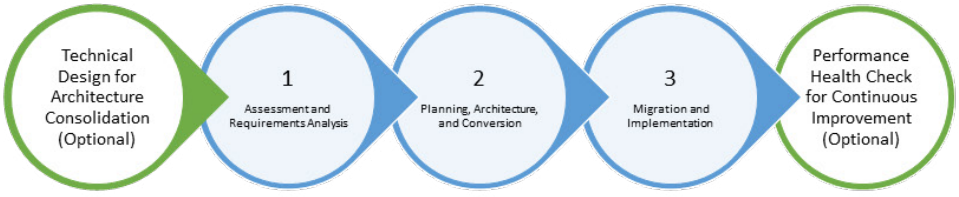
Safely Migrate From Legacy Technologies

Introduction

Doing anything the first time can be challenging, but with repetition comes mastery. The same principle applies to technology. Many organizations don't have expertise in technology migrations or are up against tight deadlines to make changes. At Fortinet, every year we help thousands of organizations safely and efficiently migrate from legacy firewalls. Our proven methodologies and expert upfront planning reduce risk, and because our experts have experience with multiple vendors, they can translate capabilities and configurations to preserve and expand protection.

Reduce Risk With Proven Migration Methodology

Proper planning, testing, and execution can mitigate some of the risks that accompany technology changes. Our professional service consultants use strict methodologies and tools to facilitate a configuration conversion. Working closely with security administrators, we determine the best approach for a successful migration. Our proven migration methodology is made up of three main steps.



1. Assessment and Requirements Analysis

The success of any migration project depends on a clear understanding of requirements and objectives. In this phase, Fortinet migration experts work with the customer to clearly define technical requirements, which include both configuration and design elements. We perform a full review of the existing configuration and identify opportunities for policy optimization. This phase concludes with a common understanding of the project objectives, timing, and migration approach.

2. Planning, Architecture, and Conversion

In this phase, our experts use automation tools such as FortiConverter to facilitate the conversion of legacy firewall configuration files. The new ruleset is then manually verified and reviewed with the customer's staff. After the validation is performed, the configuration is loaded onto a test firewall in FortiLabs for additional validation and testing. This phase also includes a joint review of the proposed final configuration and the transfer of product information to the customer team.

Benefits

- Use of proven methods reduces migration risks
- Application of best practices by experts with multivendor experience delivers the best results
- Modernized ruleset addresses business evolution, threat sophistication, and technology advancements
- Focused guidance and support of production cutover helps ensure a smooth transition

3. Migration and Implementation

With an agreed-to configuration, the next step is the final pre-cutover validation. This process includes running a series of tests to set a baseline for the solution before migration. The customer performs the tests, which is the final step before executing the migration. Fortinet consultants can help with cutover assistance to ensure traffic is flowing and the system is behaving properly. The customer then performs post-cutover verification. After the cutover acceptance, FortiCare experts continue to be available for migration-related connectivity issues for a period of time.

Upgrade Capabilities With a FortiGate-to-FortiGate Migration

The steps are the same for a FortiGate-to-FortiGate migration. A full conversion with manual validation and consolidation of the ruleset is executed to optimize the performance of policies for the upgraded device. The migration experts review the new features included in the enhanced technology with the customer team and support cutover activities to ensure a smooth transition.

Consolidate Architecture With Technical Design Services

When updating technologies, opportunities often exist to consolidate devices. Fortinet Technical Design Services provide a vendor-agnostic assessment to identify possible areas for consolidation and create technical design documents for the new environment. These technical designs can be handed over to the FortiCare Professional Services team for implementation.

Maximize Performance With a Follow-up Health Check Service

A follow-up health check can be performed to confirm that the new device is continuing to offer improved performance and security. We recommend that the follow-up health check service be performed after an initial settle-in period. The deployment efficiency and ruleset effectiveness are reviewed to make sure the solution is performing as expected.

February 18, 2021 3:37 AM

D:\Fortinet\2021 Rebranded templates\Solution Briefs\February\FortiCare Migration Services\sb-FA-forticare-firewall-migration-services-2182021\sb-FA-forticare-firewall-migration-services-2182021

897596-0-0-EN