Secure Firewall Migration Tool FAQs

Secure Firewall Migration Tool Frequently Asked Questions

Q. What are the new features supported on the Secure Firewall migration tool for Release 3.0.1?

A. The Secure Firewall migration tool 3.0.1 now provides support for Secure Firewall 3100 series only as a destination device for migrations from Fortinet.

Q. What are the new features supported on the Secure Firewall migration tool for Release 3.0?

A. The following features are supported with release 3.0:

- Migration to Cloud-delivered Firewall Management Center.

Q. What are the new features supported on the Secure Firewall migration tool for Release 2.5.2?

A. ACL Optimization for Fortinet.

Q. What are the source and target platforms for Secure Firewall migration tool 2.3 to migrate policies?

A. The Secure Firewall migration tool can now migrate policies from the supported Fortinet firewall platform to the threat defense platform. For more information, see Supported Platforms for Migration.

Q. What are the new features supported on the Secure Firewall migration tool 2.3?

A. The Secure Firewall migration tool 2.3 can migrate policies from the supported Fortinet platform to the threat defense platform.

Q. What are the supported source devices and code version?

A. You can use the Secure Firewall migration tool to migrate the configuration from Single or Multi VDOM Fortinet firewall running FortiOS 5.0 and later. For more information on the list of devices, see Supported Source Fortinet Platforms.

Q. Does Fortinet firewall support interface groups?

A. No. Fortinet firewall does not support interface groups for conversion to the threat defense.

Q. What are the features the Secure Firewall migration tool supports for migration?

A. The Secure Firewall migration tool supports migration of L3/L4 Fortinet configuration to the threat defense and can migrate the following Fortinet configurations:

- Network objects and groups (except for a few of the unsupported object types)

- Service objects, except for those service objects configured for a source and destination
- Service object groups, except for nested service object groups

Note Since nesting is not supported on the management center, the Secure Firewall migration tool expands the content of the referenced rules. The rules however, are migrated with full functionality.

- IPv4 and IPv6 FQDN objects and groups
- IPv6 conversion support (Interface, Static Routes, Objects, ACL, and NAT)
- Access rules
- NAT rules
- NAT using VIP and IP pool (Central NAT is not supported)
- Static routes and ECMP routes which are not migrated
- Physical interfaces
- Subinterfaces
- Port channels
- Zones
- Time-based objects

Q. NAT uses FQDN, which is not supported by the management center. What should I do?

A. Use of FQDN-address-object in NAT fields is not supported on Secure Firewall migration tool and management center. To replicate the same configuration as the source, you must manually, configure, post-migration, the whole set of IP addresses that are mapped with FQDN.

Q. What should I do when the source firewall has more interfaces than the target?

A. If the source firewall has more interfaces than the target, create subinterfaces on the threat defense before initiating the migration.

Q. Will the Secure Firewall migration tool migrate aggregate interfaces (port channels)?

A. The Secure Firewall migration tool does not migrate aggregate interfaces (port channels). You must configure the port channel interface on the management center before initiating the migration.

Q. What should I do with the Ignored Configuration files?

A. The Ignored configuration files contain lines that are specific to Fortinet only and are irrelevant to the management center. Hence, they are ignored. You must review the ignored configuration carefully. Any irrelevant details that reflect in the ignored section should be configured manually on the management center.

Q. I get error in the Pre-Migration Report. Can I ignore the interfaces and continue?

A. If you choose to proceed without interfaces, then the routes will also not get migrated.

Q. What are the common causes for Parse Failure?

A. Parse failure occurs if the interfaces have multiple IP addresses or IP addresses assigned with subnets, for example /32 or /128. To proceed, you must correct the IP address and retry the migration.

Q. How can I export a Fortinet configuration?

A. You can export the Fortinet configuration by extracting it from the Fortigate device or from the FortiManager if the device is managed by FortiManager. For more information, see Export the Configuration from Fortinet Networks Firewall.

Q. Is there any dependency on the management center to use the new features introduced in the Secure Firewall migration tool?

A. Yes. The Time-based Objects feature is supported with the target management center 6.6 and later.