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 Palo Alto Networks.

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 source and target platforms that the Firewall migration tool can migrate policy?
A. The Secure Firewall migration tool can migrate policies from supported PAN firewall platform to threat defense virtual platform. For more information, see Supported Source PAN Platforms.

Q. What are the hardware limitations for the conversion from PAN to Threat Defense Virtual?
A. The Secure Firewall migration tool will migrate the configuration, if the PAN OS version is 6.1.x and later.

Q. Does PAN firewall support interface groups?
A. No. PAN firewall does not support the interface groups for the conversion to threat defense virtual.

Q. NAT is using FQDN which is not supported by Management Center. What should I do?
A. As you know that FQDN in NAT is not supported on management center, in the similar line, FQDN is also not supported on Secure Firewall migration tool. To replicate, the same config as source, you must configure the whole set of IP addresses that are mapped with FQDN manually post migration.

Q. What to do when the source firewall has more interfaces than the target?
A. If the source firewall has more interfaces than the target, then, create subinterfaces on the threat defense virtual before initiating the migration.

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

Q. Is Inter VR routing supported on Management Center?
A. Any route that has Next Hop as Next VR is not supported.
Q. What is the command to extract the Route table from PAN?
A. Use the **Show routing route** command. Once you paste the route in the *txt* file, ensure that the formatting is correct. In case of multi-vsys, paste the route of the relevant *vsys* only. We recommend you to remove the tunnel, loopback, and VLAN routes from the Routing table as these interfaces are unsupported by management center.
Q. What should I do with the Ignored Configuration files?
A. The Ignored configuration contains XML tags that are specific to PAN only and is irrelevant to management center. Hence, they are ignored. You must review the ignored configuration carefully. Anything unexpected that reflects in the ignored section should be configured manually on management center.
Q. I get an error in the Pre-Migration Report. Can I ignore the interfaces and continue?
A. If you chose to proceed without interfaces, then the routes will also not get migrated.
Q. What is the common cause of 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 further, you must correct the IP address and retry the migration.
Q. Why NAT in Pre-Parsing Summary is as shown zero?
A. See Parse Summary for more information.

Q. How can you export PAN configuration?
A. The configuration must be extracted from the gateway if your device is managed by panorama. Merge the panorama configuration with the gateway and extract the configuration.

For more information, see Export the Configuration from Palo Alto Networks Firewall.

Q. What does Application Mapping do?

A. With application mapping, you can map applications to the corresponding target applications such as HTTP, SSH. You can also migrate rules that are based on application.

For more information, see Map Configurations with Applications.

Q. What happens to the policies with "application-default"?

A. Perform the following:

- If application is selected as "any" and the port is set to "application-default", then the policy is unsupported and is migrated as disabled.
- If application is selected as "xyz" and the port is set to "application-default", then the policy is migrated with application "xyz" and service as "any".