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 following features are supported with release 3.0.1:

- Migration of Enhanced Interior Gateway Routing Protocol (EIGRP) from ASA with FPS.

- Secure Firewall 3100 series is supported only as a destination device for migration.

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:

- Remote Access VPN

- Site to Site VPN pre-shared key automation

Q. What are the new features supported on the Secure Firewall migration tool for Release 2.5.1?

A. The following features are supported with release 2.5.1:

- Dynamic Routes objects

- Border Gateway Protocol

Q. What are the new features supported on the Secure Firewall migration tool for Release 2.4?

A. The following features are supported with release 2.4:

- ASA with FPS migration to threat defense.

Secure Firewall Migration Tool FAQs

Secure Firewall Migration Tool Frequently Asked Questions

• Migration of Certificate-based VPN into the management center.

Q. You have a Management Center with eight FPS security zones, FPS1 with five zones and FPS2 with three zones. ACL policies attached to FPS1 uses a combination of both FPS1 and FPS2 zones in the access rules. Will both FPS1 and FPS2 zones be migrated to threat defense?

A. The Secure Firewall migration tool will migrate FPS1 zones to threat defense zones. It will not migrate FPS2 zones. However, the source ACLs using FPS2 will be migrated partially.

Q. How will the FPS User-based ACLs be migrated?

A. The Secure Firewall migration tool does not support migration of FPS User-based ACLs to the management center. It removes the Users field and migrates the ACLs in disabled state. You must manually add the Users field and enable the ACL as part of post-migration activity on the management center.