Migrating to a New Hardware Model

https://campus.barracuda.com/doc/68357026/

The PAR file migration wizard helps you to migrate PAR files created on a supported hardware firewall to the next larger model, or a different revision of the same model. Default values and interface labels are automatically changed to fit the new model. Settings that have been modified by the admin are not migrated. The migration is available for both stand-alone and managed firewalls. There are two types of migrations:

- **Hardware upgrades to the next higher model** – For example, migrating an F80 to an F180.
- **Supported EOL models to their direct successor** – For example, migrating an F201 to an F280 Revision B.

Video

In this video we show how a standalone F280 Rev A is migrated to a F180 Rev A and a managed F300 is migrated to a F380 Rev A.

Supported EOL model migration

Source Model	Destination Models	Comment
F10	• F18 • F80	
F100 **F101**	• F80 • F180	
F200 **F201**	• F80 • F180 • F280 Rev B	
F280 Rev A	• F180 • F280 Rev B • F380	No Wi-Fi on F380

F300	• F280 Rev B • F380	
F301	• F280 Rev B • F380	No Wi-Fi on F380

Supported hardware upgrade migrations

Source Model	Destination Models	Comment
F18	• F80	
F80	• F180	
F180	• F280 Rev B	
F280 Rev B	• F380	No Wi-Fi on F380
F380	• F400	
F400	• F600	all sub models
F600	• F800	all sub models
F800	• F900	all sub models
F900	• F1000	all sub models

Migrating a stand-alone firewall to a new hardware model

Stand-alone firewalls are migrated when importing the PAR file. The firewall detects the model mismatch of the imported PAR file and guides the user through the migration process. Some configurations cannot be migrated automatically and must be verified or migrated manually by the admin before activating the migrated configuration. If you are migrating a stand-alone high availability cluster, import the PAR file on the primary firewall. The PAR file for the secondary firewall is not migrated; it is created on the primary firewall that has already been migrated.

For more information, see How to Migrate a Standalone Hardware Firewall to a new Model.

Migrating a managed firewall to a new hardware model

The configuration for managed firewalls are migrated directly on the Control Center. To ensure that no incompatible configuration changes are pushed to the remote firewall during this process, the configuration updates must be blocked. Before starting the migration, verify that the target model supports the current firmware version running on the source firewall. Some configuration nodes, such as repository linked configurations and cluster-level shared services, might have to be migrated

manually. To finish the migration, activate the configuration changes, export the PAR file, and deploy the new firewall. When the new firewall is up and installed in place of the old firewall, unblock the configuration updates.

For more information, see How to Migrate Managed Hardware Firewalls to a New Model.