Importing and Exporting Configurations

You can use the Import/Export feature to copy several types of configurations, including policies, from one appliance to another appliance of the same type. Configuration import and export is not intended as a backup tool, but can be used to simplify the process of adding new ASA FirePOWER modules.

You can import and export the following configurations:

- Access control policies and their associated network analysis, SSL, and file policies
- Intrusion policies
- System policies
- Alert responses

To import an exported configuration, both ASA FirePOWER modules must be running the same software version. To import an exported intrusion or access control policy, the rule update versions on both appliances must also match.

Note You can import policies exported from an ASA with FirePOWER services device managed by ASDM into a device managed by Firepower Management Center, provided the versions match.

Exporting Configurations

License: Any

You can export a single configuration, or you can export a set of configurations (of the same type or of different types) at once. When you later import the package onto another appliance, you can choose which configurations in the package to import.

When you export a configuration, the appliance also exports revision information for that configuration. The ASA FirePOWER module uses that information to determine whether you can import that configuration onto another appliance; you cannot import a configuration revision that already exists on an appliance.

In addition, when you export a configuration, the appliance also exports system configurations that the configuration depends on.

Tip Many list pages in the ASA FirePOWER module include an export icon next to list items. Where this icon is present, you can use it as a quick alternative to the export procedure that follows.

You can export the following configurations:

- *Alert responses* — An alert response is a set of configurations that allows the ASA FirePOWER module to interact with the external system where you plan to send the alert.
- *Access control policies* — Access control policies include a variety of components that you can configure to determine how the system manages traffic on your network. These components include access control rules; associated intrusion, file, and network analysis, and SSL policies; and objects the rules and policies use, including intrusion variable sets. Exporting an access control policy exports all settings and components for the policy except (where present) URL reputations and categories, which are equivalent across appliances and which users cannot change. Note that to import an access control policy, the rule update version on the exporting and importing ASA FirePOWER module must match.

If an access control policy that you export, or the SSL policy it invokes, contains rules that reference geolocation data, the importing module's geolocation database (GeoDB) update version is used.

- *Intrusion policies* — Intrusion policies include a variety of components that you can configure to inspect your network traffic for intrusions and policy violations. These components are intrusion rules that inspect the protocol header values, payload content, and certain packet size characteristics, and other advanced settings.

Exporting an intrusion policy exports all settings for the policy. For example, if you choose to set a rule to generate events, or if you set SNMP alerting for a rule, or if you turn on the sensitive data preprocessor in a policy, those settings remain in place in the exported policy. Custom rules, custom rule classifications, and user-defined variables are also exported with the policy.

Note that if you export an intrusion policy that uses a layer that is shared by a second intrusion policy, that shared layer is copied into the policy you are exporting and the sharing relationship is broken. When you import the intrusion policy on another appliance, you can edit the imported policy to suit your needs, including deleting, adding, and sharing layers.

If you export an intrusion policy from one ASA FirePOWER module to another, the imported policy may behave differently if the second ASA FirePOWER module has differently configured default variables.

Note You cannot use the Import/Export feature to update rules created by the Vulnerability Research Team (VRT). Instead, download and apply the latest rule update version; see Importing Rule Updates and Local Rule Files.

- *System policies* — A system policy controls the aspects of an ASA FirePOWER module that are likely to be similar to other ASA FirePOWER modules in your deployment, including time settings, SNMP settings, and so on.

Note Depending on the number of configurations being exported and the number of objects those configurations reference, the export process may take several minutes.

To export one or more configurations:

Step 1 Make sure that the ASA FirePOWER module where you are exporting the configurations and the ASA FirePOWER module where you plan to import the configurations are running the same version. If you are exporting an intrusion or access control policy, make sure that the rule update versions match.

If the versions of the ASA FirePOWER module (and, if applicable, the rule update versions) do not match, the import will fail.

Step 2 Select **Configuration** > **ASA FirePOWER Configuration** > **Tools** > **Import Export**.

The Import/Export page appears, including a list of the configurations on the ASA FirePOWER module. Note that configuration categories with no configurations to export do not appear in this list.

Tip You can click the **collapse** icon next to a configuration type to collapse the list of configurations. Click the expand folder icon next to an configuration type to reveal configurations.

Step 3 Select the check boxes next to the configurations you want to export and click **Export**.

Step 4 Follow the prompts to save the exported package to your computer.

Importing Configurations

License: Any

After you export a configuration from an ASA FirePOWER module, you can import it onto a different module as long as that module supports it.

Depending on the type of configuration you are importing, you should keep the following points in mind:

- You must make sure that the ASA FirePOWER module where you import a configuration is running the same version as the ASA FirePOWER module you used to export the configuration. If you are importing an intrusion or access control policy, the rule update versions on both appliances must also match. If the versions do not match, the import will fail.

Note You can import policies exported from an ASA with FirePOWER services device managed by ASDM into a device managed by Firepower Management Center, provided the versions match.

- If you import an access control policy that evaluates traffic based on zones, you must map the zones in the imported policy to zones on the importing ASA FirePOWER module. When you map zones, their types must match. Therefore, you must create any zone types you need on the importing ASA FirePOWER module before you begin the import. For more information about security zones, see Working with Security Zones.
- If you import an access control policy that includes an object or object group that has an identical name to an existing object or group, you must rename the object or group.
- If you import an access control policy or an intrusion policy, the import process replaces existing default variables in the default variable set with the imported default variables. If your existing default variable

set contains a custom variable not present in the imported default variable set, the unique variable is preserved.

- If you import an intrusion policy that used a shared layer from a second intrusion policy, the export process breaks the sharing relationship and the previously shared layer is copied into the package. In other words, imported intrusion policies do not contain shared layers.

Note You cannot use the Import/Export feature to update rules created by the Vulnerability Research Team (VRT). Instead, download and apply the latest rule update version; see Importing Rule Updates and Local Rule Files.

Because you can export several configurations in a single package, when you import the package you must choose which configurations in the package to import.

When you attempt to import a configuration, your ASA FirePOWER module determines whether that configuration already exists on the appliance. If a conflict exists, you can:

- keep the existing configuration,
- replace the existing configuration with a new configuration,
- keep the newest configuration, or
- import the configuration as a new configuration.

If you import a configuration and then later make a modification to the configuration on the destination system, and then re-import the configuration, you must choose which version of the configuration to keep.

Depending on the number of configurations being imported and the number of objects those configurations reference, the import process may take several minutes.

To import one or more configurations:

Step 1 Make sure that the ASA FirePOWER module where you are exporting the configurations and the module where you plan to import the configurations are running the same version. If you want to import an intrusion or access control policy, you must also make sure that the rule update versions match.

If the versions of the ASA FirePOWER module (and, if applicable, the rule update versions) do not match, the import will fail.

Step 2 Export the configurations you want to import; see Exporting Configurations, on page 1.

Step 3 On the appliance where you want to import the configurations, select **Configuration** > **ASA FirePOWER Configuration** > **Tools** > **Import Export**.

The **Import Export** page appears.

Tip Click the **collapse** icon next to a configuration type to collapse the list of configurations. Click the expand folder icon next to a configuration type to reveal configurations.

Step 4 Click **Upload Package**.

The **Upload Package** page appears.

Step 5 You have two options:

- Type the path to the package you want to upload.
- Click **Upload File** to locate the package.

Step 6 Click **Upload**.

The result of the upload depends on the contents of the package:

- If the configurations and rule versions in the package exactly match versions that already exist on your appliance, a message displays indicating that the versions already exist. The appliance has the most recent configurations, so you do not need to import them.
- If there is an ASA FirePOWER module or (if applicable) rule update version mismatch between your appliance and the appliance where the package was exported, a message appears, indicating that you cannot import the package. Update the ASA FirePOWER module or the rule update version and attempt the process again.
- If the package contains any configurations or rule versions that do not exist on your appliance, the Package Import page appears. Continue with the next step.

Step 7 Select the configurations you want to import and click **Import**.

The import process resolves, with the following results:

- If the configurations you import do not have previous revisions on your ASA FirePOWER module, the import completes automatically and a success message appears. Skip the rest of the procedure.
- If you are importing an access control policy that includes security zones, the Access Control Import Resolution page appears. Continue with step 8.
- If the configurations you import do have previous revisions on your appliance, the Import Resolution page appears. Continue with step 9.

Step 8 Next to each incoming security zone, select an existing local security zone of a matching type to map to and click **Import**.

Return to step 7.

Step 9 Expand each configuration and select the appropriate option:

- To keep the configuration on your appliance, select **Keep existing**.
- To replace the configuration on your appliance with the imported configuration, select **Replace existing**.
- To keep the newest configuration, select **Keep newest**.
- To save the imported configuration as a new configuration, select **Import as new** and, optionally, edit the configuration name.

If you are importing an access control policy that includes a file policy with either the clean list or custom detection list enabled, the **Import as new** option is not available.

- If you are importing an access control policy or saved search that includes a dependent object, either accept the suggested name or rename the object. The system always imports these dependent objects as new. You do not have the option to keep or to replace existing objects. Note that the system treats objects and object groups in the same manner.

Step 10 Click **Import**.

The configurations are imported.

What to do next

After importing an access control policy with Security Intelligence feeds, you must update the Security Intelligence feeds and wait for the latest data to be downloaded before deploying the policy. Feed contents are not part of the export or import process, and this ensures that the latest feeds are always used.