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 Check Point.

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

A. 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 Check Point.

Q. What are the hardware limitations for the conversion from Check Point to threat defense?

A. If the configuration files are compatible with the Check Point Web Visualization Tool and the FMT-CP-Config-Extractor_v4.0.1-8248 Tool, you should be able to migrate the source Check Point.

Q. Can I use the configuration that is exported from Check Point r76SP and migrate it to 4100 and 6100 Firepower platforms?

A. Yes. Support for r75 to r77.30 is provided on all platforms.

The platform is supported as long as the Check Point Web Visualization Tool is available.

Q. How do you handle negated objects in rules on Check Point?

A. If the object is of Exclusion Type object/group, then the ACL conversion follows **permit** and **block** combination. This conversion is supported by ACL though a network object/group of Exclusion type is unsupported. For example, if a Check Point ACE rule has object-group of Exclusion type referred.

- If the Check Point rule action is **permit**:
  - ACE must have an action to **Deny** for the Object-Group which is referred under **<exception></exception>** XML tag, append the rule with a *Rule for Exception Object-Group* comment.
  - ACE must have an action to **Allow** for the Object-Group which is referred under the *<base></base>* XML tag, append the rule with a *Rule for Exception Object-Group* comment.
- If the Check Point rule action is **Deny/Reset**:

- ACE must have an action to **permit** for the Object-Group which is referred under **<exception></exception>** XML tag, append the rule with a "Rule for Exception Object-Group" comment.
- ACE must have an action of **Block(Deny)/Block** with **Reset(Reject)** for the Object-Group which is referred under the **<base></base>** XML tag, append the rule with a *Rule for Exception Object-Group* comment.

Q. Does the Secure Firewall migration tool support ACE with Negate Cell? If not how are those rules handled by the Secure Firewall migration tool?

A. ACEs with negate cells are not supported by the Secure Firewall migration tool and they are converted by treating the ACE as a normal ACE. These issues will be resolved in the upcoming releases.

Q. You see Failed to bind to the DB. Access denied error. What would you do?

A. Perform the following:

- Open the Check Point Gaia Console for Management Server.
- Navigate to the users and roles settings on the Gaia Console.
- Create a new username credential on the Check Point Management Server Gaia Console that has an admin role with the home directory `/home` and Shell `/etc/cli.sh` parameters.

Q. You see the parsing count as 0, when parsing the Check Point configuration through the Secure Firewall migration tool. What would you do?

A. Perform either of these steps:

Extract the *networking.txt* file using the FMT-CP-Config-Extractor_v4.0.1-8248 Tool and avoid the hand coded *networking.txt* file.

Or

There are chances that the logging is enabled for any reasons on the check point security gateway from where the outputs for the *networking.txt* file are exported. The extraneous information that is added on the *networking.txt* file causes such an issue because the logging is enabled. If so, perform the following:

- Check the *networking.txt* file.
- Fix the file by removing the appended extra logs line.
- Upload the new zip to the Secure Firewall migration tool.

Q. Can you migrate configuration from a Check Point using VSX?

A. You can export the specific policy packages pertaining to virtual systems, one virtual system at a time. For example, when you export the configuration using the Web Visualization Tool (r75–r77.30), it exports the policy elements for all the virtual system. Hence, retain only the NAT and Policy files for the Virtual System that you want to migrate along with the *index.xml*, *communities.xml*, *network_objects.xml*, and *networking.txt* (from the Security Gateway for the policy that gets migrated) to make it a complete configuration.

For r80, select the policy package for a particular Virtual System when you connect to the Check Point Security Manager through Live Connect that you want to migrate during step 5 when you select the Check Point policy package and derive the configuration.

When you also connect to the Check point Security Gateway, provide the correct details of the correct Check Point Virtual System Check Point Firewall Package corresponding to the Check Point Policy Package.

If you still face issues, contact Cisco TAC to create a TAC case for these failures.

Q. Can you extract the Check Point (r80) configuration manually?

A. No. It is not possible to extract the Check Point (r80) configuration manually. Use Live Connect on the Secure Firewall migration tool to derive the complete r80 configuration. When you extract the configuration using manual workarounds or using a Check Point (r80) configuration that is not configured in the Secure Firewall migration tool, the configuration is incomplete and also gets migrated as unsupported, gets migrated partially, or even results in failed migrations.

For more information, see Export the Check Point Configuration Files for r80.

Q. What are the ways to pre-stage the credentials for different Check Point (r80) deployment types?

A. You can configure the credentials, before migration, on the Check Point (r80) devices in any one of the following ways:

- Exporting from Distributed Check Point Deployment
- Exporting from Standalone Check Point Deployment
- Exporting a Check Point (r80) in a Multi-Domain Deployment

Q. I am using a Custom API port on Check Point r80 for Check Point Security Manager. What must I do to extract the configuration completely?

A. If you are using a customer API port on the Check Point Smart Manager for using Check Point API, perform these:

- Check the **Check Point Multi-Domain Deployment** check box on the **Check Point Security Manager** page of Live Connect.
- Add the IP Address of Check Point CMA and API port details if using the multi-domain deployment.
- Retain the IP Address of the Check Point Security Manager if it is a general deployment and enter the details of the Custom API Port.

Q. I have a Check Point Gateway of version r80.40 and the extraction through Live Connect is fine. But, when parsing, I get the error:"Blocked VSX Feature is UNSUPPORTED in FTD ". What must I do?

A. This error occurs as the **fw vsx stat** command is deprecated starting with Check Point r80.40. The Secure Firewall migration tool is unable to parse the values after executing the **fw vsx stat** command when parsing *networking.txt* file.

As a workaround, follow these steps:

1. Unzip the *config.zip* file.
2. Open the *networking.txt* file.

   Here is an example of the sample output:

   ```
   firewall> fw vsx stat
   Deprecated command, Please see sk144112 for alternative
   Deprecated commands: cphaprob cpinfo cplic fw ips raidconfig fwaccel
   ```

   Replace this manually as follows:

```
firewall> fw vsx stat
VSX is not supported on this platform
```

3. Select all the files and compress them to .zip extension.