Getting Started with the Secure Firewall Migration Tool

About the Secure Firewall Migration Tool

This guide contains information on how you can download the Secure Firewall migration tool and complete the migration. In addition, it provides you troubleshooting tips to help you resolve migration issues that you may encounter.

The sample migration procedure (Sample Migration: Check Point to Threat defense 2100) included in this book helps to facilitate understanding of the migration process.

The Secure Firewall migration tool converts supported Check Point configurations to a supported Secure Firewall Threat Defense platform. The Secure Firewall migration tool allows you to automatically migrate the supported Check Point features and policies to threat defense. You must manually migrate all unsupported features.

The Secure Firewall migration tool gathers Check Point information, parses it, and finally pushes it to the Secure Firewall Management Center. During the parsing phase, the Secure Firewall migration tool generates a **Pre-Migration Report** that identifies the following:

- Check Point configuration XML or JSON lines with errors
- Check Point lists the Check Point XML or JSON lines that the Secure Firewall migration tool cannot recognize. Report the XML or JSON configuration lines under error section in the **Pre-Migration Report** and the console logs; this blocks migration

If there are parsing errors, you can rectify the issues, reupload a new configuration, connect to the destination device, map the Check Point interfaces to threat defense interfaces, map security zones and interface groups, and proceed to review and validate your configuration. You can then migrate the configuration to the destination device.

Console

The console opens when you launch the Secure Firewall migration tool. The console provides detailed information about the progress of each step in the Secure Firewall migration tool. The contents of the console are also written to the Secure Firewall migration tool log file.

The console must stay open while the Secure Firewall migration tool is open and running.

Important When you exit the Secure Firewall migration tool by closing the browser on which the web interface is running, the console continues to run in the background. To completely exit the Secure Firewall migration tool, exit the console by pressing the Command key + C on the keyboard.

Logs

The Secure Firewall migration tool creates a log of each migration. The logs include details of what occurs at each step of the migration and can help you determine the cause if a migration fails.

You can find the log files for the Secure Firewall migration tool in the following location: `<migration_tool_folder>\logs`

Resources

The Secure Firewall migration tool saves a copy of the **Pre-Migration Reports**, **Post-Migration Reports**, Check Point configs, and logs in the **Resources** folder.

You can find the **Resources** folder in the following location: *<migration_tool_folder>\resources*

Unparsed File

You can find the unparsed file in the following location:

<migration_tool_folder>\resources

Search in the Secure Firewall Migration Tool

You can search for items in the tables that are displayed in the Secure Firewall migration tool, such as those on the **Optimize, Review and Validate** page.

To search for an item in any column or row of the table, click the **Search** () above the table and enter the search term in the field. The Secure Firewall migration tool filters the table rows and displays only those that contain the search term.

To search for an item in a single column, enter the search term in the **Search** field that is provided in the column heading. The Secure Firewall migration tool filters the table rows and displays only those that match the search term.

Ports

The Secure Firewall migration tool supports telemetry when run on one of these 12 ports: ports 8321-8331 and port 8888. By default, Secure Firewall migration tool uses port 8888. To change the port, update port information in the *app_config* file. After updating, ensure to relaunch the Secure Firewall migration tool for the port change to take effect. You can find the *app_config* file in the following location: *<migration_tool_folder>\app_config.txt*.

Note We recommend that you use ports 8321-8331 and port 8888, as telemetry is only supported on these ports. If you enable Cisco Success Network, you cannot use any other port for the Secure Firewall migration tool.

Notifications Center

All the notifications, including success messages, error messages, and warnings that pop up during a migration are captured in the notifications center and are categorized as **Successes**, **Warnings**, and **Errors**. You can click the 

icon on the top right corner any time during the migration and see the various notifications that popped up, along with the time they popped up in the tool.

Cisco Success Network

Cisco Success Network is a user-enabled cloud service. When you enable Cisco Success Network, a secure connection is established between the Secure Firewall migration tool and the Cisco cloud to stream usage information and statistics. Streaming telemetry provides a mechanism to select data of interest from the Secure Firewall migration tool and to transmit it in a structured format to remote management stations for the following benefits:

- To inform you of available unused features that can improve the effectiveness of the product in your network.
- To inform you of additional technical support services and monitoring that is available for your product.
- To help Cisco improve our products.

The Secure Firewall migration tool establishes and maintains the secure connection and allows you to enroll in the Cisco Success Network. You can turn off this connection at any time by disabling the Cisco Success Network, which disconnects the device from the Cisco Success Network cloud.

What's New in the Secure Firewall Migration Tool

Version	Supported Features
7.0.1	

Version	Supported Features
	This release includes the following new features and enhancements: • You can now migrate configurations from your Cisco firewalls such as ASA and FDM-managed devices and third-party firewalls to Cisco Secure Firewall 1200 Series devices. See: Cisco Secure Firewall 1200 Series • You can now update the preshared keys for more than one site-to-site VPN tunnel configuration at once. Export the site-to-site VPN table in the **Optimize, Review and Validate Configuration** page to an Excel sheet, specify the preshared keys in the respective cells, and upload the sheet back. The migration tool reads the preshared keys from the Excel and updates the table. See: Optimize, Review, and Validate the Configuration Supported migrations: All • You can now choose to ignore migration-hindering, incorrect configurations and still continue the final push of a migration. Previously, the whole migration failed even if a single object's push failed because of errors. You also now have the control to abort the migration manually to fix the error and retry migration. See: Push the Migrated Configuration to Management Center Supported migrations: All • The Secure Firewall migration tool now detects existing site-to-site VPN configurations in the target threat defense device and prompts you to choose if you want them deleted, without having to log in to the management center. You could choose **No** and manually delete them from the management center to continue with the migration. See: Optimize, Review, and Validate the Configuration Supported migrations: All • If you have an existing hub and spoke topology configured on one of the threat defense devices managed by the target management center, you could choose to add your target threat defense device as one of the spokes to the existing topology right from the migration tool, without having to manually do it on the management center. See: Optimize, Review, and Validate the Configuration Supported migrations: Secure Firewall ASA • When migrating thrid-party firewalls, you can now select threat defense devices as target, which are part of a high availability pair. Previously, you could only choose standalone threat defense devices as target devices. Supported migrations: Palo Alto Networks, Check Point, and Fortinet firewall migrations • The Secure Firewall migration tool now provides a more enhanced, intuitive demo mode, with guided migration instructions at every step. In addition, you

Version	Supported Features
	can also see versions of target threat defense devices to choose and test based on your requirements. Supported migrations: All
7.0	This release includes the following new features and enhancements: **Cisco Secure Firewall ASA to Cisco Secure Firewall Threat Defense Migration** • You can now configure a threat defense high availability (HA) pair on the target management center and migrate configurations from a Secure Firewall ASA HA pair to the management center. Choose **Proceed with HA Pair Configuration** on the **Select Target** page and choose an active and a standby device. When selecting the active threat defense device, ensure you have an identical device on the management center for the HA pair configuration to be successful. See Specify Destination Parameters for the Secure Firewall Migration Tool in the *Migrating Cisco Secure Firewall ASA to Cisco Secure Firewall Threat Defense with the Migration Tool* book for more information. • You can now configure a site-to-site hub and spoke VPN topology using threat defense devices when migrating site-to-site VPN configurations from an ASA device. Click **Add Hub & Spoke Topology** under **Site-to-Site VPN Tunnels** on the **Optimize, Review and Validate Configuration** page. See Optimize, Review, and Validate the Configuration in the *Migrating Cisco Secure Firewall ASA to Cisco Secure Firewall Threat Defense with the Migration Tool* book for more information. **Fortinet Firewall to Cisco Secure Firewall Threat Defense Migration** • You can now migrate IPv6 and multiple interface and interface zones in SSL VPN and central SNAT configurations from a Fortinet firewall to your threat defense device. See Fortinet Configuration Support in *Migrating Fortinet Firewall to Cisco Secure Firewall Threat Defense with the Migration Tool* book for more information.

Version	Supported Features
6.0.1	This release includes the following new features and enhancements: **Cisco Secure Firewall ASA to Cisco Secure Firewall Threat Defense Migration** • You can now optimize network and port objects when you migrate configurations from Secure Firewall ASA to threat defense. Review these objects in their respective tabs in the **Optimize, Review and Validate Configuration** page and click **Optimize Objects and Groups** to optimize your list of objects before migrating them to the target management center. The migration tool identifies objects and groups that have the same value and prompts you to choose which to retain. See Optimize, Review, and Validate the Configuration for more information. **FDM-managed Device to Cisco Secure Firewall Threat Defense Migration** • You can now migrate DHCP, DDNS, and SNMPv3 configurations from your FDM-managed device to a threat defense device. Ensure you check the **DHCP** checkbox and **Server**, **Relay**, and **DDNS** checkboxes on the **Select Features** page. See Optimize, Review, and Validate the Configuration for more information. **Fortinet Firewall to Cisco Secure Firewall Threat Defense Migration** • You can now migrate URL objects in addition to other object types from a Fortinet firewall to your threat defense device. Review the **URL Objects** tab in the **Objects** window in **Optimize, Review and Validate Configuration** page during migration. See Optimize, Review, and Validate the Configuration for more information. **Palo Alto Networks Firewall to Cisco Secure Firewall Threat Defense Migration** • You can now migrate URL objects in addition to other object types from a Palo Alto Networks firewall to your threat defense device. Ensure you review the **URL Objects** tab in the **Objects** window in **Optimize, Review and Validate Configuration** page during migration. See Optimize, Review, and Validate the Configuration for more information. **Check Point Firewall to Cisco Secure Firewall Threat Defense Migration** • You can now migrate port objects, FQDN objects, and object groups from a Check Point Firewall to your threat defense device. Review the **Objects** window in **Optimize, Review and Validate Configuration** page during migration. See Optimize, Review, and Validate the Configuration for more information.

Version	Supported Features
6.0	

Version	Supported Features
	This release includes the following new features and enhancements: **Cisco Secure Firewall ASA to Cisco Secure Firewall Threat Defense Migration** • You can now migrate WebVPN configurations on your Secure Firewall ASA to Zero Trust Access Policy configurations on a threat defense device. Ensure that you check the **WebVPN** checkbox in **Select Features** page and review the new **WebVPN** tab in the **Optimize, Review and Validate Configuration** page. The threat defense device and the target management center must be running on Version 7.4 or later and must be operating Snort3 as the detection engine. • You can now migrate Simple Network Management Protocol (SNMP) and Dynamic Host Configuration Protocol (DHCP) configurations to a threat defense device. Make sure that you check the **SNMP** and **DHCP** checkboxes in the **Select Features** page. If you have configured DHCP on your Secure Firewall ASA, note that the DHCP server, or relay agent and DDNS configurations can also be selected to be migrated. • You can now migrate the equal-cost multipath (ECMP) routing configurations when performing a multi-context ASA device to a single-instance threat defense merged context migration. The **Routes** tile in the parsed summary now includes ECMP zones also, and you can validate the same under the **Routes** tab in the **Optimize, Review and Validate Configuration** page. • You can now migrate dynamic tunnels from the dynamic virtual tunnel interface (DVTI) configurations from your Secure Firewall ASA to a threat defense device. You can map them in the **Map ASA Interfaces to Security Zones, Interface Groups, and VRFs** page. Ensure that your ASA Version is 9.19 (x) and later for this feature to be applicable. **FDM-managed Device to Cisco Secure Firewall Threat Defense Migration** • You can now migrate the Layer 7 security policies including SNMP and HTTP, and malware and file policy configurations from your FDM-managed device to a threat defense device. Ensure that the target management center Version is 7.4 or later and that **Platform Settings** and **File and Malware Policy** checkboxes in **Select Features** page are checked. **Check Point Firewall to Cisco Secure Firewall Threat Defense Migration** • You can now migrate the site-to-site VPN (policy-based) configurations on your Check Point firewall to a threat defense device. Note that this feature applies to Check Point R80 or later versions, and management center and threat defense Version 6.7 or later. Ensure that the **Site-to-Site VPN Tunnels** checkbox is checked in the **Select Features** page. Note that, because this is a device-specific configuration, the migration tool does not display these configurations if you choose to **Proceed without FTD**. **Fortinet Firewall to Cisco Secure Firewall Threat Defense Migration** • You can now optimize your application access control lists (ACLs) when migrating configurations from a Fortinet firewall to your threat defense device.

Version	Supported Features
	Use the **Optimize ACL** button in the **Optimize, Review and Validate Configuration** page to see the list of redundant and shadow ACLs and also download the optimization report to see detailed ACL information.
5.0.1	This release includes the following new features and enhancements: • The Secure Firewall migration tool now supports migration of multiple transparent firewall-mode security contexts from Secure Firewall ASA devices to threat defense devices. You can merge two or more transparent firewall-mode contexts that are in your Secure Firewall ASA device to a transparent-mode instance and migrate them. In a VPN-configured ASA deployment where one or more of your contexts have VPN configurations, you can choose only one context whose VPN configuration you want to migrate to the target threat defense device. From the contexts that you have not selected, only the VPN configuration is ignored and all other configurations are migrated. See Select the ASA Security Context for more information. • You can now migrate site-to-site and remote access VPN configurations from your Fortinet and Palo Alto Networks firewalls to threat defense using the Secure Firewall migration tool. From the **Select Features** pane, select the VPN features that you want to migrate. See the Specify Destination Parameters for the Secure Firewall Migration Tool section in Migrating Palo Alto Networks Firewall to Secure Firewall Threat Defense with the Migration Tool and Migrating Fortinet Firewall to Secure Firewall Threat Defense with the Migration Tool guides. • You can now select one or more routed or transparent firewall-mode security contexts from your Secure Firewall ASA devices and perform a single-context or multi-context migration using the Secure Firewall migration tool.

Version	Supported Features
5.0	• Secure Firewall migration tool now supports migration of multiple security contexts from Secure Firewall ASA to threat defense devices. You can choose to migrate configurations from one of your contexts or merge the configurations from all your routed firewall mode contexts and migrate them. Support for merging configurations from multiple transparent firewall mode contexts will be available soon. See Select the ASA Primary Security Context for more information. • The migration tool now leverages the virtual routing and forwarding (VRF) funtionality to replicate the segregated traffic flow observed in a multi-context ASA environment, which will be part of the new merged configuration. You can check the number of contexts the migration tool has detected in a new **Contexts** tile and the same after parsing, in a new **VRF** tile in the **Parsed Summary** page. In addition, the migration tool displays the interfaces to which these VRFs are mapped, in the **Map Interfaces to Security Zones and Interface Groups** page. • You can now try the whole migration workflow using the new demo mode in Secure Firewall migration tool and visualize how your actual migration looks like. See Using the Demo Mode in Firewall Migration Tool for more information. • With new enhancements and bug fixes in place, Secure Firewall migration tool now provides an improved, faster migration experience for migrating Palo Alto Networks firewall to threat defense.
4.0.3	The Secure Firewall migration tool 4.0.3 includes bug fixes and the following new enhancements: • The migration tool now offers an enhanced **Application Mapping** screen for migrating PAN configurations to threat defense. See Map Configurations with Applications in *Migrating Palo Alto Networks Firewall to Secure Firewall Threat Defense with the Migration Tool* guide for more information.
4.0.2	The Secure Firewall migration tool 4.0.2 includes the following new features and enhancements: • Secure Firewall migration tool 4.0.2 introduces the inbuilt configuration extractor tool, which is now displayed on the **Extract Config Information** page. This eases configuration extraction and eliminates the task of downloading the extractor tool. Note that the FMT-CP-Config-Extractor tool is no longer available as a stand-alone application to download. See Export Device Configuration using Configuration Extractor for more information. • The migration tool now has an always-on telemetry; however, you can now choose to send limited or extensive telemetry data. Limited telemetry data inludes few data points, whereas extensive telemetry data sends a more detailed list of telemetry data. You can change this setting from **Settings** > **Send Telemetry Data to Cisco?**.

Version	Supported Features
4.0.1	The Secure Firewall migration tool 4.0.1 includes the following new features and enhancements: • You can now migrate Check Point R81 configuration to Secure Firewall Threat Defense. • You can now choose to add a **Virtual System ID** when connecting to the Check Point Security Gateway, for exporting configuration from a multi-domain Virtual System Extension (VSX) deployment. • You can extract configuration from a Check Point VSX version R77 by executing a few commands manually. See Export Device Configuration Using FMT-CP-Config-Extractor_v4.0-7965 Tool in the *Migrating Check Point Firewall to Threat Defense with the Migration Tool* guide for detailed information.
3.0.1	• For ASA with FirePOWER Services, Check Point, Palo Alto Networks, and Fortinet, Secure Firewall 3100 series is only supported as a destination device.
3.0	The Secure Firewall migration tool 3.0 provides support to migrate to Cloud-delivered Firewall Management Center from Check Point if the destination management center is 7.2 or later.
2.5.2	The Secure Firewall migration tool 2.5.2 provides support to identify and segregate ACLs that can be optimized (disabled or deleted) from the firewall rule base without impacting the network functionality from Check Point Firewalls. The ACL Optimization supports the following ACL types: • Redundant ACL—When two ACLs have the same set of configurations and rules, then removing the non-base ACL will not impact the network. • Shadow ACL—The first ACL completely shadows the configurations of the second ACL. **Note** Optimization is available for the Check Point only for ACP rule action. The Secure Firewall migration tool 2.5.2 supports Border Gateway Protocol (BGP) and Dynamic-Route Objects migration if the destination management center is 7.1 or later.

Version	Supported Features

2.2	• Provides support for r80 Check Point OS versions
	• Provides support for Live Connect to extract configurations from Check Point (r80) devices.
	• You can migrate the following supported Check Point configuration elements to threat defense for r80:
	  • Interfaces
	  • Static Routes
	  • Objects
	  • Network Address Translation
	  • Access Control Policies
	  • Global Policy—When you select this option, the source, and destination zones of the ACL policy are migrated as **Any** because there is no route-lookup.
	  • Zone-Based Policy—When you select this option, source, and destination zones are derived based on the predicative route-lookup through routing mechanism for the source and destination network objects or groups.
	Note
	Route-lookup is limited to Static routes and Dynamic routes (excluding PBR and NAT) only, and depending on the nature of the source and destination Network Object-Groups, this operation may result in rule explosion.
	Note
	IPv6 route-lookup for zone-based policy is unsupported.

Version	Supported Features

2.0	• The new optimization functionality in the Secure Firewall migration tool allows you to fetch the migration results quickly using the Search filters.
	• The Secure Firewall migration tool allows you to migrate the following supported Check Point configuration elements to threat defense:
	  • Interfaces
	  • Static Routes
	  • Objects
	  • Access Control Policy
	  • Global Policy—When you select this option, the source, and destination zones for the ACL policy are migrated as **Any**.
	  • Zone-Based Policy—When you select this option, source, and destination zones are derived based on the predicative route-lookup through routing mechanism for the source and destination network objects or groups.
	  Note
	  Route-lookup is limited to Static routes and Dynamic routes (excluding PBR and NAT) only, and depending on the nature of the source and destination Network Object-Groups, this operation may result in rule explosion.
	  • Network Address Translation
	• Provides support for Check Point OS versions—r75, r76, r77, r77.10, r77.20, and r77.30.

Licensing for the Secure Firewall Migration Tool

The Secure Firewall migration tool application is free and does not require license. However, the management center must have the required licenses for the related threat defense features to successfully register threat defense devices and deploy policies to it.

Platform Requirements for the Secure Firewall Migration Tool

The Secure Firewall migration tool has the following infrastructure and platform requirements:

- Runs on a Microsoft Windows 10 64-bit operating system or on a macOS version 10.13 or higher
- Has Google Chrome as the system default browser
- (Windows) Has Sleep settings configured in Power & Sleep to Never put the PC to Sleep, so the system does not go to sleep during a large migration push

- (macOS) Has Energy Saver settings configured so that the computer and the hard disk do not go to sleep during a large migration push

Requirements and Prerequisites for Threat Defense Devices

When you migrate to the management center, it may or may not have a target threat defense device added to it. You can migrate shared policies to a management center for future deployment to a threat defense device. To migrate device-specific policies to a threat defense, you must add it to the management center. As you plan to migrate your Check Point configuration to threat defense, consider the following requirements and prerequisites:

- The target threat defense device must be registered with the management center.
- The target threat defense device can be in a high availability configuration.
- The threat defense device can be a standalone device or a container instance. It must **not** be part of a cluster.
  - The target native threat defense device must have at least an equal number of used physical data or port channel interfaces or subinterfaces (excluding 'management-only') as that of the Check Point; if not you must add the required type of interface on the target threat defense device. Subinterfaces are created by the Secure Firewall migration tool that are based on physical or port channel mapping.
- If the target threat defense device is a container instance, at minimum it must have an equal number of used physical interfaces, physical subinterfaces, port channel interfaces, and port channel subinterfaces (excluding ‘management-only’) as that of the Check Point; if not you must add the required type of interface on the target threat defense device.

Note

- Subinterfaces are not created by the Secure Firewall migration tool, only interface mapping is allowed.
- Mapping across different interface types is allowed, for example: physical interface can be mapped to a port channel interface.

Check Point Configuration Support

Supported Check Point Configurations

- Interfaces (Physical, VLAN, and Bond interfaces)
- Network objects and groups: Secure Firewall migration tool supports migrating all the Check Point network objects to the threat defense
- Service objects
- Network Address Translation
- IPv6 conversion support (Interface, Static Routes, and Objects) and except zone-based ACLs with IPv6

- Access rules that are applied globally and support to convert Global ACLs to Zone-based ACLs
- Static routes, except for the routes configured with scope as local, and with logical interfaces as the egress interface for a static route without the next-hop IP address
- ACL with an additional logging type
- Policy-based site-to-site VPN for Check Point R80 and later versions: IPv4 and preshared key (PSK)-based authentication. We recommend that you use the **Live Connect** option to migrate VPN configurations.

Note For the ACEs configured in Check Point that have corresponding NAT rules in Check Point, the Secure Firewall migration tool does not map the real IP addresses against the translated IP addresses in the corresponding migrated ACE rules. Secure Firewall migration tool does not map the IP addresses because of the lack of reference information for the ACE rule against the NAT rule. So, during the validation of the migrated ACE and NAT configuration on the management center, you must validate and manually make changes to the ACE rules corresponding to the threat defense packet flow.

Note Though the Secure Firewall migration tool does not migrate service objects (configured with a source and destination, and a port combination with the same type of object that is called in an object group), referenced ACL rules are migrated with full functionality.

For more information on Unsupported Check Point Configuration, see Unsupported Check Point Configuration.

Partially Supported Check Point Configurations

The Secure Firewall migration tool partially supports the following Check Point configurations for migration. Some of these configurations include rules with advanced options that can be migrated without those options. If the management center supports those advanced options, you can configure them manually after the migration is complete.

- Static routes with rank and ping parameters are partially migrated.
- Bond interface with mode, XOR, active backup, round-robin types are partially migrated to LACP type in management center by the Secure Firewall migration tool.
- Alias interface configurations part of parent interfaces like physical or bond Interface, alias interface configuration in ignored and parent interface attributes are migrated as is.
- Network object group of type exclusion is supported through an ACL to keep the meaning intact.
- ACL with Add logging type and ACL with Time range.

Unsupported Check Point Configurations

The Secure Firewall migration tool does not support the following Check Point configurations. If these configurations are supported in the management center, you can configure them manually after the migration is complete.

- Alias, Bridge, 6IN4 tunnel, loopback, and PPPoE interfaces
- Network objects and groups:

- UTM-1 Edge gateway
- Check Point host
- Gateway cluster
- Externally Managed Gateways or Hosts
- Open Security Extension (OSE) device
- Logical servers
- Dynamic objects
- VoIP domains
- Zone
- CP security gateway
- CP management server
- Network Object group of the exclusion type

- Service objects:
  - RPC
  - DCE-RPC
  - Compound TCP
  - GTP
  - Other Check Point Specific service objects

- ACL policies with:
  - Unsupported ACE action types (Client Auth, Session Auth, User Auth, and other custom authentication types) are migrated with the Allow action type, but in a disabled state
  - Identity-based ACL policies
  - Zone-based policy with IPv6 route-lookup
  - User-based access control policy rules
  - Global Multi-Domain System rules cannot be migrated

Note The configurations from the Global Multi-domain system in Check Point multi-domain deployment cannot be exported. Hence the configurations pertaining to specific CMAs can only be exported and migrated.

- Objects with an Unsupported ICMP type and code
- Tunneling protocol-based access control policy rules

- Implied ACL rules
- ACE with negate parameters
- Zones for ACE when zone-based ACE is selected and has the range object with value more than 100 is migrated and are marked as **Any** with no-lookup that is appended to the ACE name and appropriate comment
- Zone for ACE with IPv6 address when zone-based ACE selected is marked as **Any** and the ACE unsupported with an appropriate comment.

Unsupported NAT Rules

The Secure Firewall migration tool does not provide support for the following NAT rules:

- Auto NAT rules that hide behind the gateway
- Manual NAT rule using Check Point Security Gateway.
- Manual NAT rule containing Network Objects with Dual Type IP Address
- Manual NAT rules containing an object-group of which the inherited object has IPv6 configuration
- Manual NAT rule with a service group
- IPv6 NAT rules

Unsupported Static Routes

- Static routes when no egress interface is found in **netstat -rnv**
- Static routes that have the logical gateway as exit interface
- Static routes of ECMP types
- Static routes that have the local scope attribute as exit interface

Guidelines and Limitations

During conversion, the Secure Firewall migration tool creates a one-to-one mapping for all supported objects and rules, whether they are used in a rule or policy. However, the Secure Firewall migration tool provides an optimization feature, that allows you to exclude migration of unused objects (objects that are not referenced in any ACLs).

The Secure Firewall migration tool deals with unsupported objects and rules as specified:

- Unsupported objects and routes are not migrated.
- Unsupported ACL rules are migrated as disabled rules into the management center.

Check Point Configuration Limitations

Migration of the source Check Point configuration has the following limitations:

- The system configuration is not migrated.

- Live Connect of Firewall is supported only for Check Point (r80) and later versions.
- All the Security Policies that are explicit (available in `Security_Policy.xml` for r77.30 and earlier versions and under Security Policy File for r80 and later versions) are migrated to the ACP on the management center. The rules on a Check Point Smart dashboard are not migrated because implied rules are not part of the exported configuration.

Note

- For Check Point (r80) and later versions, if there is a separate Application Layer Policy attached to the L4 Security Later Policy, the Secure Firewall migration tool migrates them as **unsupported**. Also, in such cases, there will be two files with ACE configurations: one for the security layer and the other for the application layer. The Secure Firewall migration tool migrates based on the priority information available in the access layer, in the *index.json* of the configuration zip file.
- For Check Point versions r80 and later, which have the Multi-Domain Deployment setup, and, which have a Global Policy along with Customer-Managed Add-on (CMA) specific policy, the order in which the Secure Firewall migration tool migrates the Check Point configuration will be slightly different from the order in the source configuration. Also, in such cases, there will be two files with ACE configurations: one for the Global Policy, and the other for the CMA policy. ACEs configured under the Domain Layer will be migrated as **unsupported**.
- The definition of the order of ACE rules, configured for a CMA that has Action as the Domain Layer in the multi-domain system, is incomplete in the extracted configuration. So, if you have a Global policy attached to a specific CMA policy in the source configuration, validate the rule number index in the extracted configuration to ensure that it is in the correct order.

- Some of the Check Point configurations, such as Dynamic Routing and VPN to threat defense cannot be migrated using the Secure Firewall migration tooll. Migrate these configurations manually.
- Check Point bridge, tunnel, and alias interfaces to management center cannot be migrated.
- Nested service object-groups or port group are not supported on the management center. As part of conversion, the Secure Firewall migration tool expands the content of the referenced nested object-group or port group.
- The Secure Firewall migration tool splits the service objects or groups with source and destination ports that are configured within the same object. References to such access control rules are converted into management center rules with the exact same meaning.

Check Point Migration Guidelines

The migration of the Check Point log option follows the best practices for threat defense. The log option for a rule is enabled or disabled based on the source Check Point configuration. For rules with **drop** or **reject** action, the Secure Firewall migration tool configures logging at the beginning of the connection. If the action is **permit**, the Secure Firewall migration tool configures logging at the end of the connection.

Object Migration Guidelines

Service objects, which are called port objects in the threat defense have different configuration guidelines for objects. For example, one or more service objects can have the same name in Check Point with one object name in lowercase and the other object name in uppercase. But, each object must have a unique name, regardless of the case as in the threat defense. The Secure Firewall migration tool analyzes all Check Point objects and handles their migration to threat defense in one of the following ways:

- Each Check Point object has a unique name and configuration. The Secure Firewall migration tool migrates the objects successfully without changes.
- The name of a Check Point service object includes one or more special characters that are not supported by management center. The Secure Firewall migration tool renames the special characters in the object name with a "_" character to meet the management center object naming criteria.
- A Check Point service object has the same name and configuration as an existing object in management center. The Secure Firewall migration tool reuses the management center object for the threat defense configuration and does not migrate the Check Point object.
- A Check Point service object has the same name but a different configuration than an existing object in the management center. The Secure Firewall migration tool reports object conflict and allows you to resolve the conflict by adding a unique suffix to the name of the Check Point Service object for migration purposes.
- Multiple Check Point service objects have the same name but in different cases. The Secure Firewall migration tool renames such objects to meet the threat defense object naming criteria.

Guidelines and Limitations for Threat Defense Devices

As you plan to migrate your Check Point configuration to threat defense, consider the following guidelines and limitations:

- If there are any existing device-specific configurations on the threat defense such as routes, interfaces, and so on, during the push migration, the Secure Firewall migration tool cleans the device automatically and overwrites from the Check Point configuration.

Note To prevent any undesirable loss of device (target threat defense) configuration data, we recommend you to manually clean the device before migration.

  During migration, the Secure Firewall migration tool resets the interface configuration. If you use these interfaces in policies, the Secure Firewall migration tool cannot reset them and hence the migration fails.

- The Secure Firewall migration tool can create subinterfaces on the native instance of the threat defense device based on the Check Point configuration. Manually create interfaces and port channel interfaces on the target threat defense device before starting migration. For example, if your Check Point configuration is assigned with the following interfaces and port channels, you must create them on the target threat defense device before the migration:
  - Five physical interfaces
  - Five port channels
  - Two management-only interfaces

Note For container instances of threat defense devices, subinterfaces are not created by the Secure Firewall migration tool, only interface mapping is allowed.

Supported Platforms for Migration

The following Check Point and threat defense platforms are supported for migration with the Secure Firewall migration tool. For more information about the supported threat defense platforms, see Cisco Secure Firewall Compatibility Guide.

Note The Secure Firewall migration tool supports migration of standalone mode or distributed Check Point configuration to a standalone threat defense device only.

Supported Target Threat Defense Platforms

You can use the Secure Firewall migration tool to migrate a source Check Point configuration to the following standalone or container instance of the threat defense platforms:

- Firepower 1000 Series
- Firepower 2100 Series
- Secure Firewall 3100 Series
- Firepower 4100 Series
- Secure Firewall 4200 Series
- Firepower 9300 Series that includes:
  - SM-24
  - SM-36
  - SM-40
  - SM-44
  - SM-48
  - SM-56
- Threat Defense on VMware, deployed using VMware ESXi, VMware vSphere Web Client, or vSphere standalone client
- Threat Defense Virtual on Microsoft Azure Cloud or AWS Cloud

Note

- For pre-requisites and pre-staging of threat defense virtual in Azure, see Getting Started with Secure Firewall Threat Defense Virtual and Azure.
- For pre-requisites and pre-staging of threat defense virtual in AWS Cloud, see Threat Defense Virtual Prerequisites.

For each of these environments, once pre-staged as per the requirements, the Secure Firewall migration tool requires network connectivity to connect to the management center in Microsoft Azure or AWS Cloud, and then migrate the configuration to the management center in the Cloud.

Note The pre-requisites of pre-staging the management center or threat defense virtual is required to be completed before using the Secure Firewall migration tool, to have a successful migration.

Note The Secure Firewall migration tool requires network connectivity to any devices hosted in the cloud to either extract the source configuration (CP (r80) Live Connect) or migrate the manually uploaded configuration to the management center in the cloud. Hence, as a pre-requisite, IP network connectivity is required to be pre-staged before using the Secure Firewall migration tool.

Supported Target Management Center for Migration

The Secure Firewall migration tool supports migration to threat defense devices managed by the management center and cloud-delivered Firewall Management Center.

Management Center

The management center is a powerful, web-based, multi-device manager that runs on its own server hardware, or as a virtual device on a hypervisor. You can use both On-Prem and Virtual management center as a target management center for migration.

The management center should meet the following guidelines for migration:

- The Management Center software version that is supported for migration, as described in Supported Software Versions for Migration, on page 23.
- The management center software version that is supported for migration for Check Point is 6.2.3.3 and later.
- You have obtained and installed smart licenses for threat defense that include all features that you plan to migrate from the Check Point interface, as described in the following:
  - The Getting Started section of Cisco Smart Accounts on Cisco.com.
  - Register the Firewall Management Center with the Cisco Smart Software Manager.

- Licensing the Firewall System
- You have enabled management center for REST API.

  On the management center web interface, navigate to **System** > **Configuration** > **Rest API Preferences** > **Enable Rest API** and check the **Enable Rest API** check box.

Important You need to have an administrator user role in management center to enable REST API. For more information on management center user roles, see User Roles.

Cloud-Delivered Firewall Management Center

The cloud-delivered Firewall Management Center is a management platform for threat defense devices and is delivered via Cisco Security Cloud Control (formerly, Cisco Defense Orchestrator). The cloud-delivered Firewall Management Center offers many of the same functions as a management center.

You can access the cloud-delivered Firewall Management Center from Security Cloud Control. Security Cloud Control connects to cloud-delivered Firewall Management Center through the Secure Device Connector (SDC). For more information about cloud-delivered Firewall Management Center, see Managing Cisco Secure Firewall Threat Defense Devices with Cloud-Delivered Firewall Management Center.

The Secure Firewall migration tool supports cloud-delivered Firewall Management Center as a destination management center for migration. To select the cloud-delivered Firewall Management Center as destination management center for migration, you need to add the Security Cloud Control region and generate the API token from Security Cloud Control portal.

Security Cloud Control Regions

Security Cloud Control is available in three different regions and the regions can be identified with the URL extension.

Table 1: Security Cloud Control Regions and URL

Region	Security Cloud Control URL
Europe	https://eu.manage.security.cisco.com/
US	https://us.manage.security.cisco.com/
APJC	https://apj.manage.security.cisco.com/
Australia	https://au.manage.security.cisco.com/
India	https://in.manage.security.cisco.com/

Supported Software Versions for Migration

The following are the supported Secure Firewall migration tool, Check Point and threat defense versions for migration:

Supported Secure Firewall Migration Tool Versions

The versions posted on software.cisco.com are the versions formally supported by our engineering and support organizations. We strongly recommend you download the latest version of Secure Firewall migration tool from software.cisco.com.

Supported Check Point Versions

The Secure Firewall migration tool supports migration to threat defense that is running Check Point OS version r75-r77.30 and r80-r80.40. Select the appropriate Check Point version in the **Select Source** page.

The Secure Firewall migration tool supports migration from the Check Point Platform Gaia and Virtual System Extension (VSX) deployments.

Supported Management Center Versions for source Check Point Firewall Configuration

For Check Point firewall, the Secure Firewall migration tool supports migration to a threat defense device managed by a management center that is running version 6.2.3.3 or later.

Note The migration to 6.7 threat defense device is currently not supported. Hence, migration may fail if the device is configured with data interface for management center access.

Supported Threat Defense Versions

The Secure Firewall migration tool recommends migration to a device that is running threat defense version 6.5 and later.

For detailed information about the Cisco Firewall software and hardware compatibility, including operating system and hosting environment requirements, for threat defense, see the Cisco Firewall Compatibility Guide.