Migrating Check Point Firewall to Cisco Secure Firewall Threat Defense Using Firewall Migration Manager

Firewall Migration Manager
Updated October 15, 2026

© 2026 Cisco Systems, Inc. All rights reserved.

Abbreviated Cisco Trademarks

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

Topics included

1 About Firewall Migration Manager.....5
Overview of Firewall Migration Manager.....6
Features in Firewall Migration Manager.....7
Default home page of Firewall Migration Manager.....10

2 Migration Requirements.....11
License requirements.....12
Platform requirements.....12
Device requirements.....12
Supported platforms and versions.....13
Firewall Management Center requirements.....14
Supported Check Point configurations for migration.....14
Guidelines for migrating Check Point firewall configurations.....17
Download the Firewall Migration Manager.....19

3 Check Point Firewall to Firewall Threat Defense Migration Workflow.....21
Check Point firewall to Firewall Threat Defense migration workflow.....22
Migrate Check Point r80-r82 using Firewall Migration Manager.....22
Import the Check Point configuration files for r80-r82.....23
Connect to Firewall Management Center and select a target device.....26
Map source configurations to the target device.....27
Migrate Check Point r75-r77 using Firewall Migration Manager.....28
Export the configuration using Check Point Web Visualization Tool.....29
Review and validate the migration configuration.....30
Review the Firewall Migration Manager pre-migration report.....33
Review the Firewall Migration Manager post-migration report.....34

1 About Firewall Migration Manager

Topics:

- Overview of Firewall Migration Manager
- Features in Firewall Migration Manager
- Default home page of Firewall Migration Manager

Introduces the Firewall Migration Manager application and explains how it facilitates the migration process from Check Point firewall to Secure Firewall Threat Defense configurations.

Overview of Firewall Migration Manager

Learn how to use the Firewall Migration Manager to automate and streamline the migration of Check Point firewall configurations to Cisco Secure Firewall Threat Defense.

The Firewall Migration Manager is a network security application that automates the migration of supported Check Point firewall configurations to Cisco Secure Firewall Threat Defense. It parses source configurations, maps features, pushes policies to the Firewall Management Center, and streamlines the migration process for organizations seeking to upgrade their firewall solutions.

Why choose Firewall Migration Manager

Firewall migration may appear simple during planning, but execution is often complicated. Common challenges include configuration dependencies, parsing timeouts on large rule sets, and unexpectedly tight cutover windows. For many organizations these risks delay their security modernization efforts.

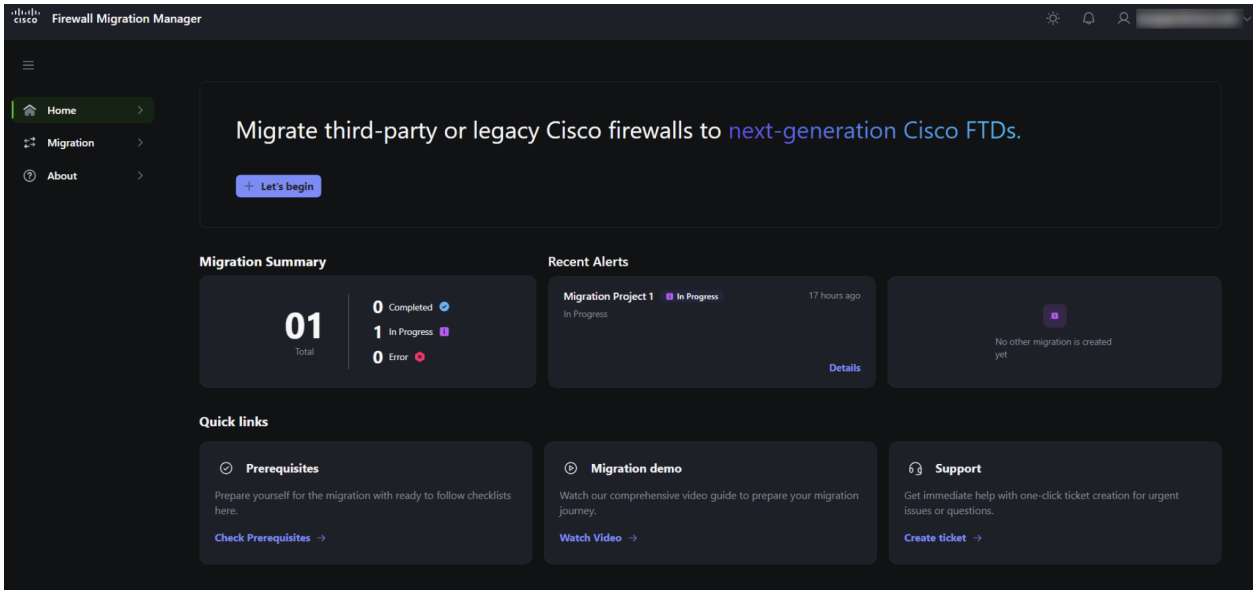
The Firewall Migration Manager an enterprise-ready product built for overcoming these challenges and to migrate seamlessly. The product helps customers and partners by offering predictable timelines, resilient workflows, and clear visibility at every stage of migration to Cisco Secure Firewall Threat Defense. As a result, migration becomes a strategic accelerator rather than a source of friction.

Key features

- **Migration efficiency**: Firewall Migration Manager streamlines and accelerates the firewall migration process while maintaining accuracy and reliability.
- **Improvised GUI**: Use Firewall Migration Manager to replace fragmented manual workflows with a guided, wizard-driven orchestration, visual task tracking, parallel execution, and proactive status monitoring.
- **Pre-deployment validation and testing**: Allows teams to fully evaluate a migration plan before committing to deployment.
- **Enhanced reporting and traceability**: Provides richer migration reports and clearer audit trails, so every stakeholder—from the engineer running the job to Cisco reviewers—has the necessary visibility.
- **Broader platform coverage**: Cisco will continue to expand supported migration sources to include more platforms, helping more teams consolidate onto Cisco Secure Firewall Threat Defense.

Dashboard overview

The Firewall Migration Manager dashboard is a centralized management interface for tracking and troubleshooting network device migrations. It also provides visibility into the health and progress of migration projects.



Key functional areas:

- **Migration monitoring:** The **Migration Summary** tile provides a real-time status overview of all migration tasks and displays counts of completed, in progress, and blocked tasks.
- **Issue identification:** The **Recent Alerts** section helps you diagnose issues. It flags failed migration tasks, identifies the exact stage and cause of failure, and provides a brief explanation of the cause, such as configuration syntax issues or connectivity timeouts.
- **Resource and support hub:** The **Quick links** section provides immediate access to essential onboarding and troubleshooting resources, including:
  - **Prerequisites**: Review the checklist to confirm all prerequisites are met before starting a migration.
  - **Migration demo**: Watch the comprehensive video that guides you through your migration journey.
  - **Support**: Get immediate help with one-click ticket creation for urgent issues or questions.

Features in Firewall Migration Manager

Learn about the new features introduced in Firewall Migration Manager, including automated workflows, centralized dashboard monitoring, and intelligent configuration parsing. These features streamline the migration of legacy firewall configurations to Secure Firewall Threat Defense, improving visibility and efficiency throughout your transition process.

This table summarizes the new features in Firewall Migration Manager.

Release	Features	Details
10.1.0	Support for Check Point firewall to Firewall Threat Defense migration.	Firewall Migration Manager supports migration of the Check Point firewall configurations to a Firewall Threat Defense device.
	Support for Fortinet firewall to Firewall Threat Defense migration.	Firewall Migration Manager supports migration of the Fortinet firewall configurations to a Firewall Threat Defense device.

Release	Features	Details
10.0.1	Support for Palo Alto Networks Firewall to Firewall Threat Defense migration.	Firewall Migration Manager supports migration of the Palo Alto Networks Firewall configurations to a Firewall Threat Defense device.
	Enhanced pre-migration and post-migration reports.	Firewall Migration Manager offers enhanced pre-migration and post-migration reports for improved user experience and easier analysis of migrated configurations.
	Support for migration from layer 2 to layer 3 interfaces.	Firewall Migration Manager supports migration from layer 2 to layer 3 interfaces by converting compatible interface configurations to routed interfaces on the Firewall Threat Defense device.
	Support for VRF migration	Firewall Migration Manager offers migration support for VRFs.
	Support for BGP migration	Firewall Migration Manager offers migration support for BGP.
	Mapping of NAT zones based on the routing table	Firewall Migration Manager uses the routing table to derive NAT zone mappings during migration.
	Handling multiple IP addresses across interfaces	During migration, if a Palo Alto Networks Firewall interface has multiple IP addresses, the Firewall Migration Manager wizard prompts you to choose one IP address for the interface.
	Migration of policy hierarchy from Panorama	Firewall Migration Manager migrates the Palo Alto Networks Firewall policy hierarchy as nested access control policies in a Firewall Threat Defense device.
	Migration of external dynamic lists	Firewall Migration Manager supports migration of external dynamic lists.
	Support for bulk addition of applications in access policy rules.	Firewall Migration Manager supports bulk addition of applications in access policy rules during migration. This reduces the manual effort required to update application-based access policies after migration.

Release	Features	Details
10.0.0	Support for ASA to Firewall Threat Defense migration.	Firewall Migration Manager supports the migration of ASA configurations to a Firewall Threat Defense device.
	Auto-detection of target versions	Automatically identifies target device version and information for Firewall Management Center and Firewall Threat Defense to ensure accurate configuration alignment.
	Automated migration workflow	The Firewall Migration Manager reduces manual effort with automated transition of security policies, network objects, and device configurations from your existing environment to a Firewall Threat Defense device.
	Centralized dashboard support	The Firewall Migration Manager dashboard provides a unified, intuitive interface to streamline your migration journey. Designed to improve visibility and operational efficiency, the dashboard offers these capabilities: • Migration overview: Monitor the status of all your migration projects in real-time and include counts for completed, in-progress, and error-state migrations. • Proactive alerting: Stay informed with immediate visibility into recent migration alerts and project details. • Quick links: Access critical resources directly from the dashboard, including pre-migration checklists, comprehensive video guides, and one-click support ticket creation. This centralized approach simplifies the transition from third-party or legacy firewalls to next-generation Cisco firewall platforms, ensuring a more organized streamlined migration process.
	Improved GUI	The Firewall Migration Manager offers an improved graphical user interface that unifies migration tasks in a wizard-driven orchestration platform. It prioritizes visual clarity, parallel task processing, and proactive status monitoring.
	Intelligent parsing	This feature automatically scans your configurations to identify items that are either unsupported or unreferenced. This helps you save time by focusing your manual cleanup efforts only on the items that require attention. This application parses enterprise-scale configurations efficiently, handling thousands of rules in minutes.
	Migration history retention	

Release	Features	Details
		Keeps migration history across different projects so you can track and revisit previous migrations.
	Parallel migration support	To improve efficiency, this feature allows you to run up to 10 migration processes simultaneously, enabling bulk handling of your network transitions.
	Pause and resume	The Firewall Migration Manager allows tasks to be paused and resumed at any point without data loss. **In-Progress** can be accessed from the **Recent Alerts** tile on the home page or by clicking **Migration** under the main menu.

Default home page of Firewall Migration Manager

Learn how to navigate the Firewall Migration Manager home page to monitor migration status, view recent alerts, access demonstration videos, and request technical support. This overview explains the primary dashboard components and provides guidance on interpreting migration status updates.

After you log in, the Firewall Migration Manager home page is displayed.

The home page has these main areas:

- **Migration summary**: Displays the total number of migrations performed, completed, in progress, and migrations that failed due to errors.
- **Recent Alerts**: Provides real-time status updates for migration tasks. The tile displays the migration project name, migration status, timestamp, and a brief description of the current phase or any action required.
- **Quick links**:
  - **Prerequisites**: Prepare yourself for the migration with ready to follow checklists.
  - **Migration demo**: Provides links to demonstration videos that highlight important capabilities and enhancements introduced in the latest release.
  - **Support**: Offers a one-click ticket creation process for immediate assistance via the **Create ticket** link.

Table 1: Migration Status

Status	Description	Action
In-progress	The migration task is currently active. The description displayed indicates the specific step being executed.	Users can monitor the progress and wait for the migration to complete. Click the **Details** link to go to the migration page.
Completed	The migration task has finished successfully.	None
Error	The migration task has failed.	Click the **Details** link to investigate the specific log or configuration issue causing the error.

2 Migration Requirements

Topics:

- License requirements
- Platform requirements
- Device requirements
- Supported platforms and versions
- Firewall Management Center requirements
- Supported Check Point configurations for migration
- Guidelines for migrating Check Point firewall configurations
- Download the Firewall Migration Manager

Lists the licensing, platform, device, and configuration requirements for migrating from Check Point firewall to Firewall Threat Defense using the Firewall Migration Manager.

License requirements

Understand the licensing requirements for Firewall Migration Manager and the Firewall Management Center.

While the Firewall Migration Manager is free and does not need a license, ensure that you must meet these licensing requirements:

- Firewall Threat Defense devices must have required entitlements for the features that you plan to use.

  The feature licenses can be Essentials, Malware, Intrusion Prevention System (IPS), Carrier, URL Filtering, or Secure Client licenses.

- If you have a virtual Firewall Management Center, you must have a license for Firewall Management Center Virtual.

  The required number of Firewall Management Center Virtual licenses depends on how many devices it manages.

For more information about Firewall Management Center, refer to the Licenses section of *Cisco Secure Firewall Management Center Administration Guide*.

Platform requirements

Lists the supported operating systems, browser, and power management settings required for successful Firewall Migration Manager migrations.

The Firewall Migration Manager requires specific platform and configuration settings for proper operation. The supported environments and necessary settings are:

- **System requirements**:
  - Microsoft Windows 11 64-bit or later
  - macOS 14 or later

  You need an internet connection to connect to Cisco.com.

  > **Note**
  >
  > If you want to perform migration in an air-gapped or isolated environment without internet access, contact Cisco TAC to obtain the air-gapped Firewall Migration Manager installer.

- **Power management (Windows):**: Set **Sleep** settings in **Power & Sleep** to **Never put the PC to sleep** during migration to prevent interruptions.
- **Power management (macOS)**: Configure **Energy Saver** settings so that the computer and hard disk remain active throughout the migration process.

Device requirements

Learn about the device requirements and prerequisites for migrating Check Point firewall configurations to Firewall Threat Defense.

When you migrate to the Firewall Management Center, it is not mandatory to have a target Firewall Threat Defense device added to it. You can migrate policies to a Firewall Management Center for future deployment to a Firewall Threat Defense device.

If a Firewall Threat Defense device is added to the Firewall Management Center, before starting migration, ensure your target Firewall Threat Defense device meets these criteria:

- **Registration**: The target Firewall Threat Defense device must be registered with the Firewall Management Center.
- **Configuration state**:
  - Supports high availability (HA) configurations.
  - Supports standalone or container instances.
- **Restriction**: The target Firewall Threat Defense device must not be part of a device cluster.
- **Interface mapping**:
  - If using container instances, the Firewall Threat Defense device must have a minimum interface count (physical, sub-interfaces, and port channels) equal to or greater than the source Check Point firewall device.
  - The Firewall Migration Manager supports mapping across different interface types such as physical interfaces to port channel interfaces.

> **Note**
>
> The Firewall Migration Manager does not create sub-interfaces for target multi-instance Firewall Threat Defense devices. You must pre-configure them on the target device.

> **Warning**
>
> During the push migration, the Firewall Migration Manager automatically cleans and overwrites existing device-specific configurations (routes, interfaces, and so on). We highly recommend that you manually clean the device prior to the migration to avoid unintended data loss.

Supported platforms and versions

Explains the minimum hardware and software requirements needed for successful migration of Check Point firewall to Firewall Threat Defense using Firewall Migration Manager.

For a successful migration, ensure that your hardware and software versions align with these specifications:

Component	Minimum Supported Version
Source Gaia OS	R75 - R77 and R80+ versions Live Connect is supported only for Check Point (r80-r82)
Firewall Management Center	6.2.3.3 and later

Component	Minimum Supported Version
Target Firewall Threat Defense	6.2 and later

Supported target devices

- **Physical**: Firepower 1000, 2100, 4100, 9300 (SM modules), and Secure Firewall 220, 1200, 3100, 3200, 4200, 6100 series
- **Virtual**: Threat Defense on VMware (ESXi/vSphere) and Cloud (Azure/AWS).

Firewall Management Center requirements

Lists the prerequisites for using on-premises Firewall Management Center for Firewall Migration Manager.

The Firewall Migration Manager supports only the on-premises Firewall Management Center.

- Smart Licensing: License requirements on page 12
- REST API:

  You must enable REST API (**System** (⚙) > **Configuration** > **REST API Preferences**).

  > **Note**
  >
  > You must have an administrator user role in Firewall Management Center to enable REST API.

Supported Check Point configurations for migration

Lists fully, partially, and unsupported Check Point firewall configurations for migration

The Firewall Migration Manager categorizes Check Point configurations based on feature parity with a Firewall Threat Defense device.

Fully supported configurations

- ACL inline layers
- Cluster shared interfaces
- Interfaces (physical, VLAN, and bond interfaces)
- Network objects and groups, and service objects
- Network Address Translation
- Manual NAT rule containing network objects with dual type IP address
- IPv6 address conversion support (interface, static routes, and objects) and except zone-based ACLs with IPv6 address
- 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
- ACE with negate parameters
- Policy-based site-to-site VPN: IPv4 and preshared key (PSK)-based authentication.
- Identity-based ACL policies
- User-based access control policy rules

Note

- For Check Point access control entries (ACEs) with corresponding NAT rules, Firewall Migration Manager does not map real IP addresses to translated IP addresses in the migrated ACE rules. The migration cannot map these addresses because the ACE rules do not include reference information for the related NAT rules.

  When you validate the migrated ACE and NAT configuration in Firewall Management Center, review the ACE rules and update them manually to match the Firewall Threat Defense device packet flow. Firewall Migration Manager changes the DNAT destination IP address in an access rule.
- Firewall Migration Manager 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.
- Though Firewall Migration Manager 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.

Partially supported configurations

Firewall Migration Manager partially supports these Check Point configurations for migration:

- Static routes with rank and ping parameters
- Bond interface with mode, XOR, active backup, round-robin types are partially migrated to LACP type in Firewall Management Center.
- 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.

Some of these configurations include rules with advanced options that can be migrated without those options. If the Firewall Management Center supports those advanced options, you can configure them manually after the migration is complete.

Unsupported configurations

Firewall Migration Manager does not support these Check Point configurations.

- Alias, bridge, tunnel, 6in4 tunnel, loopback, and PPPoE interfaces
- Dynamic routing

- Route-based VPN
- 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
  - CP security gateway
  - CP management server
  - Network object group of the exclusion type
- Service objects:
  - Remote Procedure Call (RPC)
  - Distributed Computing Environment Remote Procedure Call (DCE-RPC)
  - Compound TCP
  - GPRS Tunneling Protocol (GTP)
  - Other Check Point-specific service objects

  Nested service object groups or port group are not supported in Firewall Management Center. Firewall Migration Manager expands the referenced nested object group or port group.
- 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
  - Zone-based policy with IPv6 route-lookup
- Objects with an unsupported ICMP type and code
- Tunneling protocol-based access control policy rules
- Implied ACL rules

  The rules on a Check Point Smart dashboard are not migrated because implied rules are not part of the exported configuration.
- Remote Access VPN
- Zone for ACE with IPv6 address when zone-based ACE selected is marked as Any and the ACE unsupported with an appropriate comment.

If these configurations are supported in the Firewall Management Center, you can configure them manually after the migration is complete.

Unsupported NAT rules

Firewall Migration Manager does not support these NAT rules:

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

Unsupported static routes

Firewall Migration Manager does not support these 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 for migrating Check Point firewall configurations

Lists the guidelines for migrating Check Point firewall configurations.

Review these guidelines before migrating the Check Point firewall configurations.

General guidelines

- Live Connect is supported only for Check Point R80+ versions.
- During migration, Firewall Migration Manager creates a one-to-one mapping for all supported objects and rules, whether they are used in a rule or policy. However, Firewall Migration Manager provides an optimization feature that allows you to exclude migration of unused objects (objects that are not referenced in any ACLs).
  - Unsupported objects and routes are not migrated.
  - Unsupported ACL rules are migrated as disabled rules to the Firewall Management Center.
- For Check Point versions r80-r82 and later in a multi-domain deployment, the extracted configuration might not include the complete rule order for access control entry (ACE) rules when a Customer Management Add-on (CMA) policy uses a Domain Layer action.

  If the source configuration has a Global policy attached to a specific CMA policy, review the rule number index in the extracted configuration and verify that the rules are in the correct order.
- The log option for a rule is enabled or disabled based on the source Check Point firewall configuration.

  For rules with **drop** or **reject** action, Firewall Migration Manager configures logging at the beginning of the connection. If the action is **permit**, Firewall Migration Manager configures logging at the end of the connection.
- Firewall Migration Manager 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 Firewall Management Center rules with the exact same meaning.

Object migration guidelines

Review these guidelines for service objects, which are called port objects in a Firewall Threat Defense device.

In Check Point firewall configurations, service object names can differ only by case. For example, one object name can use lowercase letters and another can use uppercase letters. In Firewall Threat Defense devices, each port object name must be unique, regardless of letter case.

Firewall Migration Manager analyzes all Check Point firewall objects and handles their migration to the Firewall Threat Defense device in one of these ways:

- If each Check Point firewall object has a unique name and configuration, Firewall Migration Manager migrates the objects successfully without changes.
- If the name of a Check Point firewall service object includes one or more special characters that are not supported by Firewall Management Center, Firewall Migration Manager renames the special characters in the object name with a "_" character to meet the Firewall Management Center object naming criteria.
- If a Check Point firewall service object has the same name and configuration as an existing object in Firewall Management Center, Firewall Migration Manager reuses the Firewall Management Center object for the Firewall Threat Defense device configuration and does not migrate the Check Point object.
- If a Check Point firewall service object has the same name but a different configuration than an existing object in the Firewall Management Center, Firewall Migration Manager reports object conflict and allows you to resolve the conflict by adding a unique suffix to the name of the Check Point firewall service object for migration purposes.
- If multiple Check Point firewall service objects have the same name but in different cases, Firewall Migration Manager renames such objects to meet the Firewall Threat Defense device object naming criteria.

Firewall Threat Defense guidelines

- If there are any existing device-specific configurations on the Firewall Threat Defense such as routes, interfaces, and so on, during the push migration, Firewall Migration Manager cleans the device automatically and overwrites from the Check Point firewall configuration.

  > **Note**
  >
  > To prevent any undesirable loss of device configuration data from the Firewall Threat Defense device, we recommend you to manually clean the device before migration.

  During migration, Firewall Migration Manager resets the interface configuration. If you use these interfaces in policies, Firewall Migration Manager cannot reset them and the migration will fail.

- Firewall Migration Manager can create subinterfaces on the native instance of the Firewall Threat Defense device based on the Check Point firewall configuration. Manually create interfaces and port channel interfaces in the target Firewall Threat Defense device before starting migration.

  For example, if your Check Point firewall configuration is assigned with these interfaces and port channels, you must create them in the target Firewall Threat Defense device before migration:

  - Five physical interfaces
  - Five port channels
  - Two management-only interfaces

> **Note**
>
> For container instances of Firewall Threat Defense devices, subinterfaces are not created by the Firewall Migration Manager, only interface mapping is allowed.

Download the Firewall Migration Manager

Learn how to download the Firewall Migration Manager on your local Windows or macOS system.

Before you begin

- Ensure you have administrative rights to install Firewall Migration Manager on your local machine.
- You must have a Windows 11 64-bit machine or macOS version 14 or later, with internet connectivity to Cisco.com.

> **Note**
>
> If you want to perform migration in an air-gapped or isolated environment without internet access, contact Cisco TAC to obtain the air-gapped Firewall Migration Manager installer.

Procedure

1. Browse to Cisco Software Download Center and click Firewall Migration Manager.
2. Download the most recent version of the Firewall Migration Manager.

   Ensure that you download the executable file of Firewall Migration Manager for Windows or macOS machines.

3 Check Point Firewall to Firewall Threat Defense Migration Workflow

Topics:

- Check Point firewall to Firewall Threat Defense migration workflow
- Migrate Check Point r80-r82 using Firewall Migration Manager
- Migrate Check Point r75-r77 using Firewall Migration Manager
- Review and validate the migration configuration
- Review the Firewall Migration Manager pre-migration report
- Review the Firewall Migration Manager post-migration report

Guides you through the complete workflow for migrating Check Point firewall configurations to a Firewall Threat Defense device.

Check Point firewall to Firewall Threat Defense migration workflow

Learn how to migrate your Check Point firewall configurations to Firewall Threat Defense using the Firewall Migration Manager. This workflow covers configuration gathering, parsing, mapping, and validating configurations to ensure a successful transition to your destination device.

Summary

Firewall Migration Manager automates the Check Point firewall configuration migration by ensuring accurate parsing, validation, and deployment of Check Point firewall configurations to a Firewall Threat Defense device.

Workflow

These stages describe how the Check Point firewall to Firewall Threat Defense device migration works:

1. **Gather and parse configuration**: Firewall Migration Manager collects information from the Check Point firewall and parses its configuration.
   - Firewall Migration Manager connects to the Check Point Security Gateway to collect the network configurations of the firewall.
   - Firewall Migration Manager connects to the Check Point Security Manager to collect the object and VPN configurations, and policy packages of the firewall.
2. **Connect to the Firewall Management Center and select the Firewall Threat Defense**: Firewall Migration Manager connects to the Firewall Management Center and allows you to choose the required Firewall Threat Defense.
3. **Map Check Point Firewall interfaces, security zones, and applications to the Firewall Threat Defense**: Firewall Migration Manager maps interfaces, security zones, interface groups, and applications of the Check Point firewall to the Firewall Threat Defense device. You must review and validate the mapping.
4. **Review pre-migration report**: Firewall Migration Manager generates a report that identifies unsupported, ignored, and erroneous configurations, including blocking errors and the reasons for them.
5. **Remediate parsing errors**: Firewall Migration Manager highlights parsing errors so that you can resolve them before migration.
6. **Push validated configuration**: Firewall Migration Manager pushes the validated configuration to the Firewall Management Center and migrates the configuration to the destination device.
7. **Review post-migration report**: Firewall Migration Manager generates a detailed report, covering fully migrated, partially migrated, or not migrated configurations. It lists fixes, identifies changes made to avoid conflicts, shows any skipped items, and documents migration failures or manual requirements.

Migrate Check Point r80-r82 using Firewall Migration Manager

Guides you through the process of migrating Check Point r80-r82 using Firewall Migration Manager

Before you begin

- Download the latest version of Firewall Migration Manager from Cisco Software Download Center.
- Ensure that you review all the Migration Requirements on page 11.
- For large configuration files, disable system sleep settings before you start the migration.

Procedure

1. In Firewall Migration Manager, from the left pane, click **Migration** ( ), and click **Start new migration** on the top-right of the window.

   The migration workflow is initiated. Alternatively, you can click **Lets Begin** in the home page to start the migration.

2. Import the Check Point configuration files for r80-r82 on page 23.
3. For **Select Access Control Policy**, choose one of these options:
   - **Global policy**: Select global policy to migrate all the policies as global policies. The source and destination zones are marked as **Any** for these policies.
   - **Zone-based policy**: Select zone-based policies to populate source and destination zones through predictive analysis with route lookup. The analysis supports only static and dynamic routes; it does not consider policy-based routing (PBR) or NAT.

     Depending on the source and destination network objects and groups, this option can increase the number of rules.

     Note

     If the source configuration has inline layers, then you must select zone-based policy migration.

4. Connect to Firewall Management Center and select a target device on page 26.
5. Map source configurations to the target device on page 27.
6. Review and validate the migration configuration on page 30.
7. Review the Firewall Migration Manager pre-migration report on page 33.
8. Review the Firewall Migration Manager post-migration report on page 34.

Import the Check Point configuration files for r80-r82

Procedure

1. In Firewall Migration Manager, from the left pane, click **Migration** ( ), and click **Start new migration** on the top-right of the window.

   The migration workflow is initiated. Alternatively, you can click **Lets Begin** in the home page to start the migration.

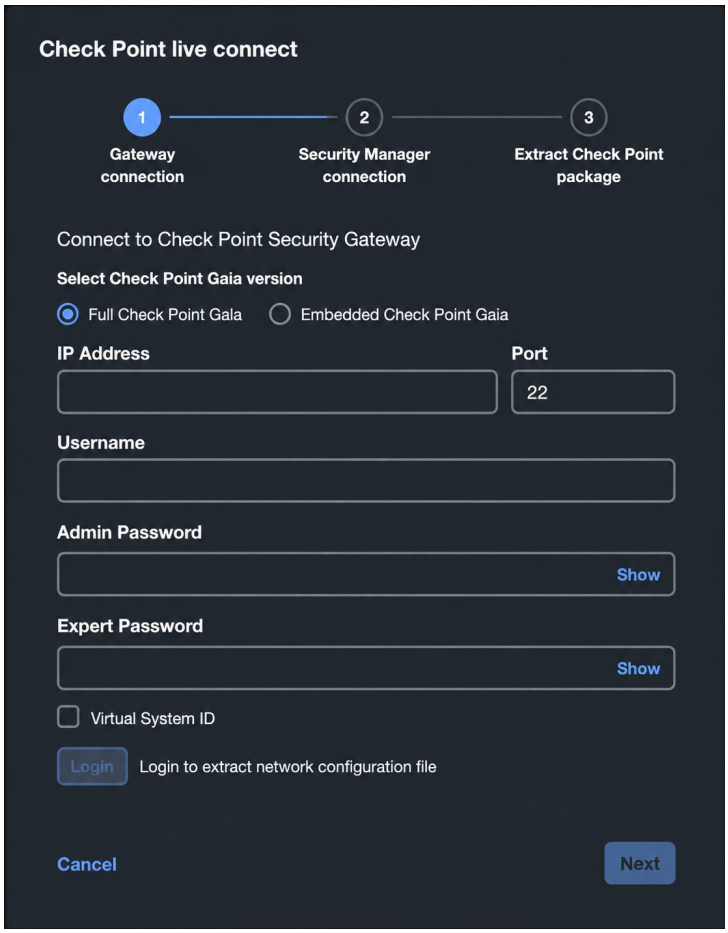
2. In **Select Firewalls**, from the **Select source** drop-down list, choose **Check Point (r80-r82)**.
3. For **Select configuration extraction method**, choose one of these options:
   - **Manual**: Upload a configuration file directly to the Firewall Migration Manager.
   - **Live Connect**: Connect to the Check Point Security Gateway and the Check Point Security Manager and extract the configuration files.

> **Note**
>
> Live Connect is the mandatory option to import the configuration files.

4. Click **Live Connect** and click **Check Point live connect**.

   Firewall Migration Manager first connects to the Check Point Security Gateway and then to the Check Point Security Manager.

5. Connect to the **Check Point Security Gateway**.



   a) Select a Check Point Gaia version:

      - **Full Check Point Gaia**
      - **Embedded Check Point Gaia**

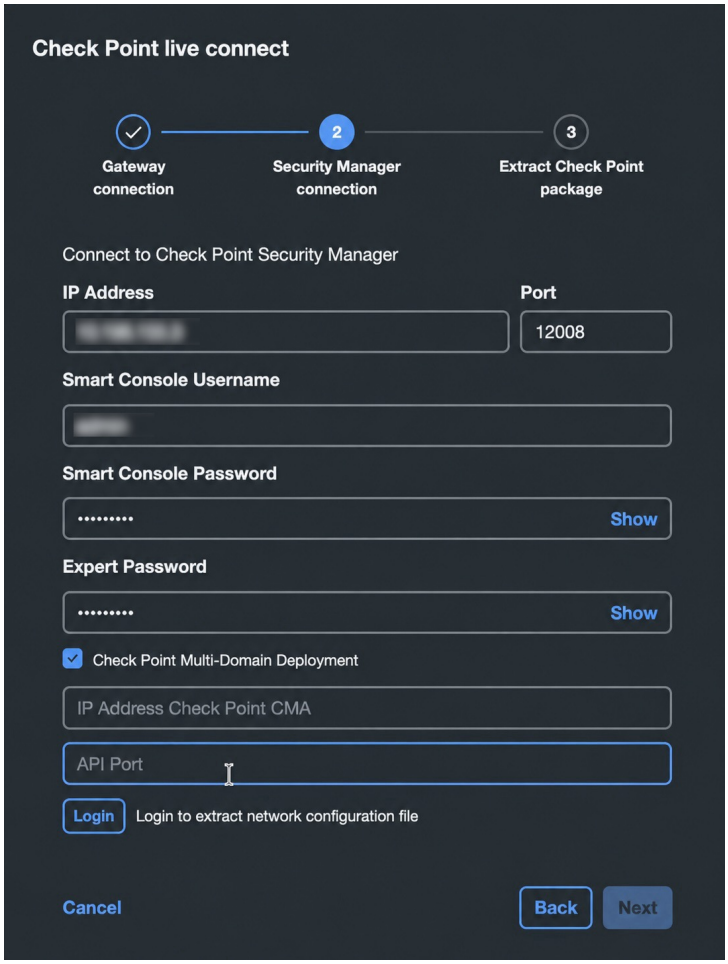
   b) Configure these parameters:

      - **IP address**
      - **Port**
      - **Username**
      - **Admin Password**

- **Expert Password**

c) Check the **Virtual System ID** check box, if required.
d) Click **Login** to log into the Check Point Security Gateway and extract the network configurations of the Check Point firewall.
e) Click **Next**.

6. Connect to the **Check Point Security Manager**.



a) Configure these parameters:

- **IP address**
- **Port**
- **Smart Console Username**
- **Smart Console Password**
- **Expert Password**

b) Check the **Check Point Multi-Domain Deployment** check box, if the Check Point Security Gateway and a Check Point Security Manager are in a multi-domain deployment setup.
c) Click **Login** to log into the Check Point Security Manager and extract the object and VPN configurations of the Check Point firewall.
d) Click **Next**.

7. From the **Select Package** drop-down list, choose a Check Point package and click **Start Extraction**.

8. Click **Finish**.
9. Click **Download configurations** to get the configurations of the Check Point firewall, and click **Proceed**.

Connect to Firewall Management Center and select a target device

Connect to Firewall Management Center, and select a target device for the Check Point firewall migration.

Before you begin

1. Obtain the credentials of the target Firewall Management Center.
2. If you need to apply an intrusion policy or file policy to an access control list (ACL) in the **Review and Validate** page, create the policy in Firewall Management Center before migration.

   Firewall Migration Manager retrieves policies from the connected Firewall Management Center. Reusing an existing policy helps avoid performance issues and migration push failures that can occur when you create and assign a new policy to multiple ACLs.
3. Start the migration workflow.
4. Import the Check Point firewall configuration files.

Procedure

1. In **Target Information**, choose a Firewall Management Center from the **Select target** drop-down list.
2. Enter the IP address, hostname, or FQDN of the Firewall Management Center and click **Connect**.

   You can only migrate to the devices available in the selected domain.
3. In the **Login to target FMC** dialog box, enter the username and password, and click **Login**.

   Firewall Migration Manager logs in to the Firewall Management Center and retrieves a list of managed devices.
4. In **Device Selection**, you can choose one of these actions:
   - Click **Select FTD** to choose a single Firewall Threat Defense device or an HA pair.
   - Click **Migrate shared configurations** to migrate only the shared configurations without selecting a Firewall Threat Defense device. These configurations include details of access control lists, NAT, and objects.
5. If you choose the **Select FTD** option, from the **Select FTD** drop-down list, choose a Firewall Threat Defense device.

   Choose a target device that meets these requirements:
   - The device must have at least the same number of physical or port-channel interfaces as the source configuration.
   - The container instance must have at least the same number of physical or port-channel interfaces and subinterfaces.
   - The device must use the same firewall mode as the Check Point firewall.

   Interface names do not need to match between the source and target devices.

   After you select a device, you can view device details such as IP address, device version, device model, mode (routed or transparent), and multi-instance state.
6. Click **Next**.

What to do next

Map source configurations to the target device on page 27

Map source configurations to the target device

Map source configurations to the target device by assigning interfaces, security zones, interface groups, and applications, with options for automatic or manual mapping and validation to ensure accurate migration.

Firewall Migration Manager retrieves a list of interfaces of the source and target device, and maps them according to their identities. For example, 'management-only' interfaces are mapped automatically and cannot be changed.

Before you begin

1. Start the migration workflow.
2. Import the Check Point firewall configuration files.
3. Connect to Firewall Management Center and select a target device on page 26

Procedure

1. In **Mappings**, click the **Interfaces** tab to map the source and target device interfaces.
   a) (Optional) Click **Auto Map** to automatically map the source and target device interfaces.

      A **Confirm Auto-Creation** pop-up window is displayed. If you click **Auto create**, Firewall Migration Manager automatically maps Check Point firewall interfaces to existing security zones and interface groups in Firewall Management Center with matching names. If no match is found, Firewall Migration Manager creates a new security zone and interface group in Firewall Management Center using the Check Point firewall interface name.

   b) To manually map the interfaces, from the **FTD interface** drop-down list, choose the interface.

      Note

      - Management-only interfaces are mapped automatically and cannot be changed.
      - Once an interface is assigned, you cannot select it again.
      - Manual mapping of physical interfaces, port-channel and sub-interfaces is required only when the target device operates in multi-instance mode.

   c) Review, validate and edit the mapping, if required.
2. Click the **Security zones** tab to map the source security zones with the Firewall Management Center security zones and interface groups.

   In Firewall Management Center, access control policies and NAT policies use interface objects. These interface objects are grouped into:

   - Security zones: An interface can belong to only one security zone.
   - Interface groups: An interface can belong to multiple interface groups.

   a) (Optional) Click **Auto Map** to automatically map the source and target device security zones.
   b) To manually map the security zones, configure:
      - From the **FMC Security Zones** drop-down list, choose a security zone.

- From the **FMC Interface Groups** drop-down list, choose an interface group.

c) To add a new security zone or interface group, click **Add Zones & Interface Groups**.
d) Click the **Security zones (SZ)** tab and in the **Add new security zone** field, enter the security zone name and click **Add**.
e) Click the **Interface groups (IG)** tab and in the **Add new interface group** field, enter the interface group name and click **Add**.
f) Click **Save & Close**.

3. Click the **Applications** tab to map the source and target device applications automatically.

   If the Firewall Migration Manager unable to map the applications, you must manually choose the application from the **Target application/Ports** field.

   Click **Validate mappings** to validate the applications.

4. Click **Next**.

What to do next

Review and validate the migration configuration on page 30

Migrate Check Point r75-r77 using Firewall Migration Manager

Guides you through importing Check Point configuration files for r80-r82 using manual upload or Live Connect.

Before you begin

- Download the latest version of Firewall Migration Manager from Cisco Software Download Center.
- Ensure that you review all the Migration Requirements on page 11.
- For large configuration files, disable system sleep settings before you start the migration.
- Export the configuration using Check Point Web Visualization Tool on page 29

Procedure

1. In Firewall Migration Manager, from the left pane, click **Migration** ( ), and click **Start new migration** on the top-right of the window.

   The migration workflow is initiated. Alternatively, you can click **Lets Begin** in the home page to start the migration.

2. In **Select Firewalls**, from the **Select source** drop-down list, choose **Check Point (r75-r77)**.
3. For **Select configuration extraction method**, click **Manual** to upload a configuration zip file containing communities.xml, index.xml, NAT_Policy.xml, network_objects.xml, Security_Policy.xml, services.xml, users.xml, and networking.txt.
4. For **Select Access Control Policy**, choose one of these options:
   - **Global policy**: Select global policy to migrate all the policies as global policies. The source and destination zones are marked as **Any** for these policies.
   - **Zone-based policy**: Select zone-based policies to apply route lookup for zone mapping based on static routes to access rules. If the source configuration has inline layers, zone-based policy migration is required.

     Depending on the source and destination network objects and groups, this option can increase the number of rules.

5. Click **Proceed**.
6. Connect to Firewall Management Center and select a target device on page 26.
7. Map source configurations to the target device on page 27.
8. Review and validate the migration configuration on page 30.
9. Review the Firewall Migration Manager pre-migration report on page 33.
10. Review the Firewall Migration Manager post-migration report on page 34.

Export the configuration using Check Point Web Visualization Tool

Procedure

1. Open the command prompt on the workstation that has access to the Check Point Management Server.
2. Download the Web Visualization Tool from the Check Point Portal for the Check Point firewall version.
3. Unzip the Web Visualization Tool zip file.
4. Create a new sub folder under the same root folder where you extracted the Check Point Web Visualization Tool.
5. Change to the directory where the Web Visualization Tool is stored, and run this command:

```
C:\Web_Visualisation_Tool> cpdb2web.exe [-s management_server] [-u admin_name
| -a certificate_file] [-p password] [-o output_file_path] [-t table_names]
[-c | -m gateway | -l package_names] [-gr] [-go] [-w
Web_Visualization_Tool_installation_directory]
```

For example,

```
C:\Web_Visualisation_Tool> cpdb2web.exe -s 198.51.100.1  -u admin -p admin123
 -o  Output
```

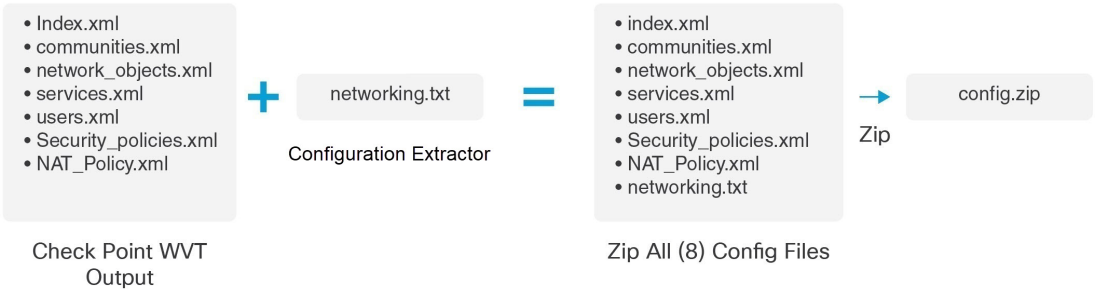
The Output directory contains seven files after you run these commands.

Command	Description
management_server	IP address of the Check Point Management Server.
admin_name	Check Point Management Server username.
password	Check Point Management Server password.
output_file_path	Relative path to store the output files.

> **Note**
>
> The name of the security policy and NAT policy file must be `Security_Policy.xml` and `NAT_Policy.xml` respectively. If the filenames are different, rename them manually.
>
> If there are multiple security and NAT policy files, ensure that you select and keep only the `Security_Policy.xml` and `NAT_Policy.xml` files of the Check Point firewall that you want to migrate.

What to do next

1. Get the networking.txt file from the Check Point Security Gateway.
2. Zip the files from the Web Visualization Tool and the networking.txt file.



Note

.tar or other compressed file types are not supported.

Review and validate the migration configuration

Review and validate the migrated Check Point firewall configuration before deployment.

Before you push the migrated Check Point firewall configuration to the Firewall Management Center, review the configuration carefully and resolve any conflicts. Firewall Migration Manager identifies issues and allows remediation. You can also associate policies such as IPS and file policies to access control rules, make changes to objects, and optimize the configuration before deployment.

Procedure

1. In the left pane of the Firewall Migration Manager click **Review**.

   If you close the Firewall Migration Manager at the **Review** page, your progress is saved and you can resume the migration later. To resume the migration, click **Migration** on the main menu, and then select the migration project name on the **Migration Projects** window.

2. Click **Download Pre-Migration Report** to review the pre-migration report.

   For more information, refer to Review the Firewall Migration Manager pre-migration report on page 33.

3. Review access control configurations.
   a. Click **Access Control** in the **Shared configurations** area
   b. Check mappings for each entry and verify them.
   c. If you do not want to migrate specific access control list policies, deselect them and from the **Bulk actions** drop-down list, click **Do not migrate**.

      Rules not chosen for migration will be grayed out.

   d. In the **Edit rule** dialog box, update the existing data or add new data.

      To add an object to source or destination:

1. Check the check box adjacent to the object in the left pane.
2. Click the **Add Source** or **Add Destination** button under the **Selected Sources** or **Selected Destination and Applications** column to move the object to the respective location.
3. Click the delete icon to delete any object from the source or destination.

> **Note**
>
> Rules that are not applicable are grayed out in the table.

e. To apply a Firewall Management Center file policy to one or more access control policies, select the policies and choose **Actions** > **File Policy**.

f. In the **File Policy** dialog box, select the appropriate file policy and apply it to the selected access control policies and click **Save**.

g. To apply a Firewall Management Center IPS policy to one or more access control policies, select the policies and choose **Actions** > **IPS Policy**.

In the **IPS Policy** dialog, select the IPS policy, its corresponding variable set, apply it to the selected access control policies and click **Save**.

h. To update the logging options for an access control rule,select the rule and choose **Actions** > **Log**.

In the **Log** dialog box, you can enable logging events either at the beginning or end of a connection or both. If you enable logging, you must opt to send the connection events either to the **Event Viewer**, to the **Syslog** or both. When you opt to send connection events to a syslog server, you can choose the syslog policies that are already configured on the Firewall Management Center from the **Syslog** drop-down menu.

i. To change actions for migrated access control rules in the Access Control table, select the rules, and choose **Actions** > **Rule Action**.

In the **Rule Action** dialog from the **Actions** drop-down, you can click the **ACP** tab.

4. Click these tabs and review the configuration items:
   - Interfaces
   - Routes (Static)
   - Access Control
   - NAT
   - Objects (Network objects, User objects, Port objects, URL objects, and VLAN objects)
   - Site-to-Site VPN

> **Note**
>
> For VPN configurations, review VPN filter configurations and extended access list objects.
>
> To exclude specific NAT rules or route interfaces from migration, deselect as needed, choose **Actions** > **Do not migrate**, and click **Save**. Excluded rules are grayed out.

a. (Optional) To rename network or port objects, in the **Network Objects** or the **Port Objects** tab, select the object and choose **Actions** > **Rename**.

   Access rules and NAT policies referencing renamed objects are updated accordingly.

b. Review routes from the **Routes** section. Select routes you do not want to migrate, and choose **Actions** > **Do not migrate**.

5. Review and validate site-to-site VPN tunnels:

   In the **Site-to-Site VPN Tunnels** section, review the VPN tunnel data from the source firewall such as **Source Interface**, **VPN Type**, and **IKEv1** and **IKEv2** configurations and provide preshared key values as needed.

6. Optional: Click **Download** to download details for each configuration item in the grid.
7. Resolve migration issues listed in the **Actions** area. Click **Remediate** to resolve the issues.

   For example, to avoid conflicts with existing Firewall Management Center objects, add a suffixe to object names. Select the object and choose **Actions** > **Add suffix** to apply the default suffix, or enter a suffix manually.

   When errors are resolved, a tick mark appears next to each error.

> **Note**
>
> Ensure that all issues are resolved before proceeding with migration.

8. Validate the configuration.

a. After you complete your review, click **Validate**. The **Begin migration** dialog box appears with the validated configurations.

b. Confirm migration by checking the confirmation box and click **Begin Migration**.

   You can close this window while migration is in progress. You will receive notifications if the migration status changes. You can resume the workflow on the main menu by selecting **Migration**, and click the migration project name.

c. Click **Next**.

9. Review migration results.

   After a successful migration, a summary and a link to the post-migration report appears.

a. Click **Download report** to download and save the post-migration report. A copy is also saved in the Resources folder.

b. If migration fails, review the post-migration report, log file, and unparsed file to troubleshoot the failure.

What to do next

Review the post-migration report.

Review the Firewall Migration Manager pre-migration report

Review the pre-migration report to identify potential migration issues and validate the migration before proceeding.

Before migration, it's important to thoroughly review the pre-migration report. This report shows errors, unreferenced configurations, ignored configuration lines, and rules that were not migrated completely.

Incomplete rules can affect the source setup, block authorized traffic, or allow unintended traffic. After migration, refine rules and policies in Firewall Management Center to optimize traffic handling and system performance.

Procedure

1. Navigate to the location where you downloaded the **Pre-migration report**.

   Note

   A copy of the pre-migration report is also saved in the `Resources` folder in the same location as the Firewall Migration Manager.

2. Open the pre-migration report and carefully review its contents to identify issues, if any, that may cause the migration to fail.

   This report contains:

   - **Overall Summary**–Lists the supported configurations from the source device that can be migrated successfully to Firewall Management Center.

     While connecting to a live Check Point firewall, the summary includes the hit count information, the number of times a rule was encountered and its timestamp information.

   - **Unsupported Configuration**–Displays details of Check Point firewall configurations that are not migrated. Review each item, and if required configure the equivalent manually before or after migration. Unsupported rules may alter the original configuration, restrict authorized traffic, or permit unwanted traffic if not addressed.

   - **Ignored Configuration**–Displays details of unsupported configuration by Firewall Management Center, or not parsed by Firewall Migration Manager because they are irrelevant to the target device. Review these and verify whether each feature is supported in Firewall Management Center. If required, configure the features manually in Firewall Management Center.

   - **Unreferenced Configuration**–Displays the details of Check Point firewall configurations defined in the source configuration but are not used in any access-group, prefix list, VPN, or policy. These items will not be migrated. Decide whether to remove them from the source or manually add them to the target device.

For more information about the supported features in Firewall Management Center and Firewall Threat Defense, refer to *Cisco Secure Firewall Management Center Device Configuration Guide*.

What to do next

After the migration, review and adjust migrated configurations as needed to optimize performance and ensure compliance.

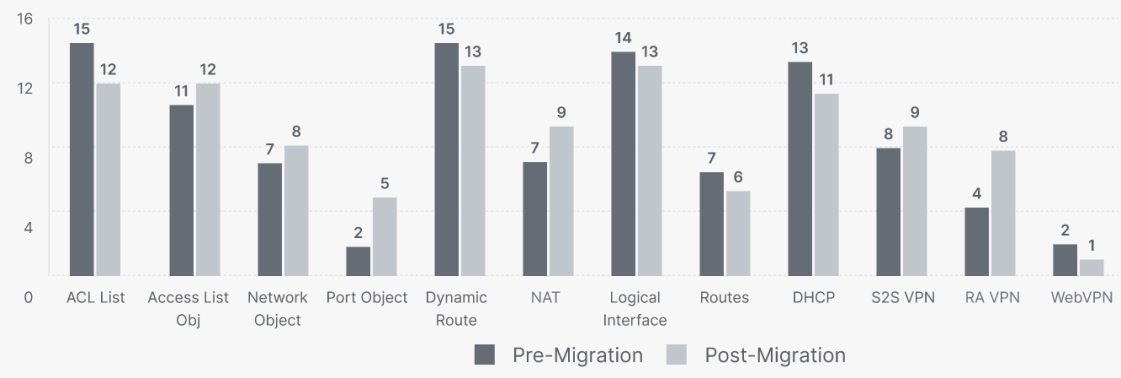
Review the Firewall Migration Manager post-migration report

Review the post-migration report to understand how your Check Point firewall configuration was migrated and identify any configurations that require manual migration.

The post-migration report provides details about the source and target devices such as policies, interface and zone mapping, ACL rules, ACL optimization, and the overall optimization performed on the configuration. It also provides details about partially migrated configurations and errors that occurred during migration. The report also offers guidance on resolving the errors.

Procedure

1. Open the **Post-migration report**.
2. Review the post-migration report:
   - **Summary Overview**–View comparison charts showing pre-migration and post-migration states.



   - **Device Details**–View summary of source and target devices.
   - **Network Mapping**
     - **Policies Selected for Migration**–Displays device configuration features that you chose to migrate. The section will display if the features were successfully migrated. It will also display the set of features that you chose not to migrate. This section helps you review the features and decide if you want to manually add the features that were not migrated in management center.
     - **Interface-to-Interface Mapping**–Displays the successfully migrated interfaces and the mappings between the source and target device interfaces.

> **Note**
>
> This section is not applicable for migrations without a destination Firewall Threat Defense device or if **Interfaces** are not selected for migration.

- Source **Interface Names to Security Zones and Interface Groups**–Displays the successfully migrated logical interfaces and how you mapped them to security zones and interface groups in a Firewall Threat Defense device. Confirm these mappings.

> **Note**
>
> This section is not applicable if **Access Control Lists** and **NAT** are not selected for migration.

- **Object & ACL Anomalies**
  - **Object Conflict Handling**–Displays objects that were split or renamed to avoid conflicts in the Firewall Management Center.
  - **ACL Category Conflict Handling**–Displays the category names that were trimmed to fit Firewall Management Center naming limits.
  - **Optimization**–Displays objects renamed to avoid conflicts, or reused where an identical object already existed in Firewall Management Center.
  - **Reused Objects**–Displays objects that the Firewall Migration Manager reused because they already existed in Firewall Management Center with an identical configuration.
  - **Access Control Rules, NAT, and Routes You Chose Not to Migrate**–Displays the rules that you chose not to migrate with the Firewall Migration Manager. Review these rules that were disabled by the Firewall Migration Manager and were not migrated. If required, you can configure these rules manually.
- **Migration Issues**
  - **Partially Migrated Configuration**–Displays partially migrated rules, including rules with unsupported advanced options. Review these rules, verify whether the advanced options are supported in Firewall Management Center, and if so, configure these options manually.
  - **Policy Rules Failing Zone Lookup**–Displays rules that could not resolve a source or destination zone during migration.
  - **Expanded Access Control Rules**–Displays access control policy rules that were expanded from a single Check Point firewall point rule into multiple Firewall Threat Defense rules during migration.
- **Action Taken on Features**
  - **Action Taken on Converted Features**–Displays VPN policies and deprecated settings that were automatically adjusted during migration.
  - **Actions Taken on Access Control Rules**
    - **Access Rules You Chose Not to Migrate**–Displays access control rules that you chose not to migrate with the Firewall Migration Manager. Review these rules. If required, configure these rules manually.

- **Access Rules with Rule Action Change**–Displays all access control policy rules that had **Rule Action** changed using the Firewall Migration Manager. Rule Action values are: Allow, Trust, Monitor, Block, Block with reset. Review these rules. If required, configure these rules manually.
- **Access Control Rules that have IPS Policy and Variable Set Applied**–Displays all access control policy rules that have IPS policies. Review these rules carefully and determine whether the feature is supported in a Firewall Threat Defense device.
- **Access Control Rules that have File Policy Applied**–Displays all access control policy rules that have File Policy applied. Review these rules carefully and determine whether the feature is supported in a Firewall Threat Defense device.
- **Access Control Rules that have Rule 'Log' Setting Change**–Displays the access control rules that had **Log setting** changed using the Firewall Migration Manager. The Log Setting values are: False, Event Viewer, Syslog. Review these rules. If required, configure these rules manually.
- **Access Control Rules that have failed Zone-lookup**–Displays access control rules that fail the route-lookup operation. The Firewall Migration Manager performs the route-lookup operation based on the route (static and connected) information in the source configuration to populate the destination security zones in the access rules.
- **Access Control Rules for Tunneled Protocols**–Displays tunnel rules that are migrated as a prefilter tunnel rule during migration.

- **Errors & Failures**–Items that failed to migrate to Firewall Management Center.

  Error report may indicate an incorrect migrated configuration or a conflict within the Firewall Management Center caused by existing configurations or unsupported features. Review each error and apply the suggested remedies. Verify the corrections before proceeding or resuming the configuration push to the target Firewall Management Center.

> **Note**
>
> - Unsupported rules are not migrated to prevent unwanted traffic from passing through the Firewall Threat Defense device. Configure a rule in Firewall Management Center to block this traffic by the Firewall Threat Defense.
> - If you need to apply an intrusion policy or file policy to an access control list (ACL) on the **Review and Validate** page, create the policy in Firewall Management Center before migration.
>
>   Firewall Migration Manager retrieves policies from the connected Firewall Management Center. Reuse the same policy to avoid performance issues and possible push failures when assigning policies to multiple targets.

For more information about supported features in Firewall Management Center and Firewall Threat Defense, refer to the Firewall Management Center Configuration Guides.

3. In Firewall Management Center, perform these actions:
   a) Review the migrated configuration for the Firewall Threat Defense device to confirm that all expected rules and other configuration items, including the following, were migrated:
      - Interfaces
      - Routes (Static)
      - Access Control
      - NAT

- Objects (Network objects, User objects, Port objects, URL objects, and VLAN objects)
- Site-to-Site VPN

b) Configure all partially supported, unsupported, ignored, and disabled configuration items and rules that were not migrated.

For information on how to configure these items and rules, refer to Firewall Management Center Configuration Guides.

4. After your review and manual configurations are complete, deploy the migrated configuration from Firewall Management Center to the Firewall Threat Defense device.

Verify that the data is reflected correctly in the **Post-Migration Report** for unsupported and partially supported rules.

The Firewall Migration Manager assigns the policies to the Firewall Threat Defense device. Verify that the changes are reflected in the running configuration. To help you to identify the policies that are migrated, the description of those policies includes the hostname of the source device configuration.