Cisco Secure Firewall Threat Defense Model Migration Guide, Version 7.4

About Secure Firewall Threat Defense Model Migration 2

Best Practices for Migration 6

Revised: September 28, 2023

About Secure Firewall Threat Defense Model Migration

The Firewall Threat Defense model migration wizard enables you to migrate device-specific and interface configurations from an old threat defense model to a new model. You can also migrate all policies assigned to the source device, except site-to-site VPN policies, to the target device.

Supported Devices for Migration

Supported Source Devices

- Cisco Firepower 1120
- Cisco Firepower 1140
- Cisco Firepower 1150
- Cisco Firepower 2110
- Cisco Firepower 2120
- Cisco Firepower 2130
- Cisco Firepower 2140

Note The source devices must be version 7.0 or later.

Supported Target Devices

- Cisco Secure Firewall 3105
- Cisco Secure Firewall 3110
- Cisco Secure Firewall 3120
- Cisco Secure Firewall 3130
- Cisco Secure Firewall 3140

Note The Cisco Secure Firewall 3110, 3120, 3130, and 3140 devices must be version 7.1 or later. Cisco Secure Firewall 3105 must be version 7.3 or later.

License for Migration

You must register and enroll the device with the smart licensing account. The migration copies the source device licenses to the target device.

Prerequisites for Migration

- You must register the source and the target devices to the management center.
- Your Smart Licensing account must have the license entitlements for the target device.
- We recommend that the target device is a freshly registered device without any configurations.
- Source and target devices must be in the same:
    - Domain
    - Firewall mode: Routed or Transparent
    - Compliance mode
- The target device must not be:
    - In a multi-instance mode
    - Part of a cluster
- The user must have modify permissions on the device.
- The configurations on the source device must be valid and have no errors.
- The source device can have pending deployments. However, deployment, import, or export tasks must not run on either of the devices during the migration.
- If the source device is part of an HA pair, the target device need not be part of an HA pair and vice versa. The migration does not form or break the HA pair.

What Configurations Does the Wizard Migrate?

The migration wizard copies the following configurations from the source device to the target device:

- Licenses
- Interface configurations
- Inline sets configurations
- Routing configurations
- DHCP and DDNS configurations
- Virtual router configurations
- Policies
- Associated objects and object overrides
- Platform settings
- Remote branch deployment configurations

The migration wizard copies the following policy configurations from the source device to the target device:

- Health policies

- NAT policies
- QoS policies
- Remote access VPN policies
- FlexConfig policies
- Access control policies
- Prefilter policies
- IPS policies
- DNS policies
- SSL policies
- Malware and File policies
- Identity policies

The migration wizard copies the following routing configurations from the source device to the target device:

- ECMP
- BFD
- OSPFv2/v3
- EIGRP
- RIP
- BGP
- Policy Based Routing
- Static Route
- Multicast Routing
- Virtual Router

The migration wizard copies the following interfaces from the source device to the target device:

- Physical interfaces
- Sub-interfaces
- Etherchannel interfaces
- Bridge group interfaces
- VTI interfaces
- VNI interfaces
- Loopback interfaces

Limitations for Migration

- The wizard does not migrate:
  - Site-to-site VPN policies
  - SNMP configurations

    After the migration, you can configure SNMP using the platform settings for the device.
- You can perform only one migration at a time.
- If the speed, auto-negotiation, and duplex settings of the source interface are valid for the mapped interface of the target device, the values are copied. If not, these parameters are set to the default values.
- Remote access VPN trustpoint certificates are not enrolled. You must manually enroll these certificates before the deployment.
- After migration, by default, the target device uses Snort 3 and not Snort 2, even if the source device uses Snort 2.
- For HA devices:
  - Target Device: You cannot map the interfaces that are part of the failover configuration. These interfaces are disabled in the wizard.
  - Source and Target Devices: The wizard does not migrate HA configurations such as monitored interfaces, failover trigger criteria, and interface MAC addresses. You must manually configure these parameters after the migration if required.

Migrate the Secure Firewall Threat Defense

Before you begin

Review the prerequisites and limitations for the migration.

Procedure

Step 1 Choose **Devices** > **Device Management**.

Step 2 Click **Migrate** on the top-right of the page.

Step 3 Click **Start** on the welcome screen.

Step 4 From the **Source Device** drop-down list, choose a device.

If the device is part of an HA pair, only the container name of the HA pair appears.

Step 5 Click **Next**.

Step 6 From the **Target Device** drop-down list, choose a device.

If the device is part of an HA pair, only the container name of the HA pair appears.

Step 7 Click **Next**.

Step 8 In the **Configure Interfaces** step, map the physical interfaces of the source device with those of the target device.

Mapping of all interfaces is not mandatory. You must map all named interfaces and interfaces that are part of other interfaces. You cannot map interfaces that are part of an HA failover configuration. These interfaces are disabled in the wizard. The wizard creates the logical interfaces according to the interface mapping provided by the user.

- Click **Map Default** to configure default interface mappings.

  For example, Ethernet1/1 in the source device will be mapped to Ethernet1/1 in the target device.

- Click **Clear All** to clear all the mappings.

Step 9 Click **Next**.

Step 10 Click **View Mappings** to verify the interface mappings.

Step 11 Click **Submit** to start the migration.

Step 12 View the migration status in the **Notifications** > **Tasks** page.

What to do next

After a successful migration, you can deploy the device.

Deployment is not mandatory, you can validate the configurations and deploy as required. However, before the deployment ensure that you perform the actions mentioned in Best Practices for Migration, on page 6.

Best Practices for Migration

After a successful migration, we recommend that you perform the following actions before the deployment:

- Change the IP addresses of the interfaces if the source device is live, as they are copied to the target device from the source device.
- Ensure that you update your NAT policies with the modified IP addresses.
- Configure the interface speeds if they are set to default values after migration.
- Re-enroll the device certificates, if any, on the target device.
- If you have a HA setup, configure HA parameters such as monitored interfaces, failover trigger criteria, and interface MAC addresses.
- Configure the diagnostic interface as it gets reset after migration.
- (Optional) Configure SNMP using the platform settings for the device.
- (Optional) Configure remote branch deployment configurations.

  If the source or target device had manager access through a data interface, after the migration, the manager access will be lost. Update the manager access configuration on the target device. For more information, see the *Change the Manager Access Interface from Management to Data* topic in the Cisco Secure Firewall Management Center Device Configuration Guide or the Online Help.

- (Optional) Configure site-to-site VPN if required. These configurations are not migrated from the source device.
- View the deployment preview before the deployment. Choose **Deploy** > **Advanced Deploy** and click the **Preview** ( ) icon for the device.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA 95134-1706
USA

Asia Pacific Headquarters
CiscoSystems(USA)Pte.Ltd.
Singapore

Europe Headquarters
CiscoSystemsInternationalBV
Amsterdam,TheNetherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.