Palo Alto Networks to Cisco Secure Firewall Threat Defense Migration Prerequisites Guide

First Published: 2025-11-14

Palo Alto Networks to Cisco Secure Firewall Threat Defense Migration Prerequisites Guide

The document provides essential information for users planning to migrate their firewall configurations from Palo Alto Networks (PAN) to Firewall Threat Defense using the Cisco Secure Firewall Migration Tool.

Pre-Migration Requirements

Before beginning the migration from Palo Alto Networks (PAN) to Firewall Threat Defense, the following conditions must be met:

1. **Stable IP Connection**: Ensure a stable connection between the Secure Firewall Migration Tool and the Firewall Management Center.
2. **Firewall Management Center Version**: The Management Center must be running version 6.2.3 or later. For optimal migration performance and enhanced software quality, use the recommended release for your Threat Defense and Management Center.

Note Refer to the gold star on Cisco Software Central for the recommended release.

3. **Firewall Management Center User Account**: Create a dedicated user account on Management Center with administrative privileges for the Firewall Migration Tool and use the credentials during migration.
4. **Firewall Threat Defense Device**: To migrate device configurations (such as interfaces, routes, etc.), add the target Firewall Threat Defense device to your Firewall Management Center before migration.

Note This step can be skipped If only shared configurations (such as objects, NAT, and ACLs) are being migrated.

5. **Palo Alto Networks Configuration Requirements**: Export a named configuration snapshot from your Palo Alto firewall in .xml format.

Important If your NAT policies use the same source and destination zone, upload the routing table in .txt format.

Feature-Specific Requirements

- **Remote Deployment**: Remote deployment is available for Firewall Management Center and Firewall Threat Defense, version 6.7 or later. If remote deployment is enabled, the Firewall Migration Tool migrates only ACLs, Network Objects, Port Objects, and NAT. You must manually migrate interfaces and route configurations on Firewall Management Center.
- **Identity-based Access Control Rules**: AD/LDAP integration with Firewall Management Center is mandatory. Additionally, you must create an identity policy in Firewall Management Center. After migration, you must attach the identity policy to the access policy prior to deploying the configuration.
- **Site-to-Site VPN Tunnel**:
  - Add Firewall Threat Defense to Firewall Management Center before migration.
  - Ensure Firewall Threat Defense and Firewall Management Center versions are 6.7 or later (support for VTI is available from version 6.7).
  - Confirm the source firewall is running version 8.0 or later.
  - All Virtual Tunnel Interface (VTI) tunnels without IP address are unsupported. You must manually migrate them after the migration process.

Note For Firewall Management Center route-based VPNs, it is mandatory to have a VTI tunnel IP address.

  - The Firewall Migration Tool will migrate VPN tunnels as a point-to-point network topology.
  - Migrate Palo Alto trust-points manually to Firewall Management Center as PKI objects before beginning Certificate-based VPN migration.

- **Remote Access VPN (RAVPN):**
  - The target Firewall Management Center version must be 7.2 or later.
  - The Firewall Threat Defense version must be 7.0 or later.
  - The source firewall configuration (PAN) must be 8.0 or later.
  - Only migration for RADIUS, LOCAL, SAML, and LDAP authentication is currently supported.
  - The Firewall Threat Defense must be added to Firewall Management Center.
  - Upload the required AnyConnect client image as part of the pre-migration activity.
  - Palo Alto trustpoints (certificates) should be manually migrated to the Firewall Management Center as PKI objects during pre-migration.

Interface Requirements

- If the source firewall contains port channel interfaces, create similar port channels on Firewall Management Center. The tool will automatically create subinterfaces.
- If migrating to an Firewall Threat Defense with a cluster interface configuration, remove the existing cluster interface configuration before using the device as the target Firewall Threat Defense. Alternatively, proceed with "No FTD Flow" to skip "Interfaces & Routes" migration.

System Requirements

- **Power Options:** Ensure that your system does not enter sleep mode during a large migration push.
- **Supported Browsers:** Google Chrome or Microsoft Edge.

Firewall Management Center Requirements

- **On-Premises Management Center:**
  - Firewall Management Center software version 6.2.3 or later.
  - Install smart licenses for Firewall Threat Defense ensuring all features that need to be migrated are included.
  - Enable the REST API on Firewall Management Center from **System** > **Configuration** > **REST API Preferences**.
  - You must have the administrator user role to enable the REST API.
- **Cloud-Delivered Firewall Management Center:** The Firewall Migration Tool supports Cloud-Delivered Firewall Management Center through Security Cloud Control (formerly Cisco Defense Orchestrator). The tool allows Cloud-Delivered Firewall Management Center to function as the destination management center.

Supported PAN Configurations

The below features are supported for PAN to Firewall Threat Defense migration in Firewall Migration Tool:

- Access control policy rules
- NAT policies (with specific limitations)
- Network objects and groups
- Service objects and groups
- Address objects and groups
- Security zones

- Static routing
- Layer 3 interfaces
- Subinterfaces
- VLAN interfaces
- Access Rule Optimization (identifies shadow and redundant rules)

  We recommend using this option.

Note Virtual wire interface will not be migrated whereas virtual wire zone will be migrated. You must manually create BVI interface on Firewall Threat Defense after migration.

Limitations for Palo Alto Networks to Cisco Secure Firewall Threat Defense Migration

This section covers configurations and scenarios with limitations or those not supported by the Firewall Migration Tool:

Unsupported PAN Configurations

The Firewall Migration Tool does not support the following features for migration from PAN to Firewall Threat Defense.

- Time-based access control policy rules
- FQDN objects that begin with or contain special characters
- Wildcard FQDNs
- NAT rule with FQDN object and FQDN object group in the translated source
- NAT rule with FQDN object and FQDN object group in both original source and destination
- NAT rule with FQDN object group in the translated destination
- IPv6 NAT
- Dynamic routing protocols (OSPF and BGP)
- VRFs
- Policies with profile source or destination negate

Note All policies (supported or unsupported) are migrated to Firewall Management Center. Unsupported policies are migrated as disabled. You must configure your system according to Firewall Management Center requirements before enabling policies.

Partially Supported PAN Configurations

The following configurations are partially supported. Some advanced options may not be migrated for the listed configurations.

- Access control policy rules using profiles.
- Service groups that contains service objects with protocols TCP, UDP, and SCTP (SCTP type will be removed).
- Object groups containing both supported and unsupported objects (unsupported objects will be removed).

VPN Features

- **Deprecated Phase-1/Phase-2 (IKE/IPsec) Parameters:** IKEv1 DH Group 2, 5; IKEv2 DH Group 2, 5, 24; Hash MD5; Encryption des, 3des, null.
- **Remote Access VPN (RAVPN) Authentication:** TACACS+ and Kerberos authentication are currently not supported.

Interface Requirements

- Migration to Firewall Threat Defense with cluster interface configuration is not supported.
- Virtual wire interface will not be migrated (whereas virtual wire zone will be migrated). You must manually create BVI interface on Firewall Threat Defense after migration.

Firewall Management Center Version

Migrating Palo Alto Networks to Firewall Threat Defense version 6.7 is currently not supported when the device uses a data interface for Firewall Management Center access.

Supported Platforms for Migration

Supported PAN Versions

The Firewall Migration Tool supports migration from PAN firewall OS version 8.0 and later.

Supported Target Firewall Threat Defense Platforms

- Firepower 1000 Series
- Firepower 2100 Series
- Secure Firewall 3100 Series
- Firepower 4100 Series
- Secure Firewall 4200 Series
- Firepower 9300 Series (SM-24, SM-36, SM-40, SM-44, SM-48, SM-56)
- Threat Defense on VMware (ESXi, vSphere)
- Threat Defense Virtual on Microsoft Azure Cloud

- Threat Defense Virtual on AWS Cloud

Supported Firewall Management Center Versions

The Firewall Migration Tool supports PAN firewall migration to Firewall Management Center version 6.2.3.3 or later.

Supported Firewall Threat Defense Versions

For PAN to Firewall Threat Defense migration, we recommend migrating to Firewall Threat Defense version 6.5 and later.

Security Cloud Control Regions

Security Cloud Control is available for below 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/

References

For detailed information and the complete migration guide, see *Migrating Palo Alto Networks Firewall to Cisco Secure Firewall Threat Defense with the Migration Tool*

Additional Resources:

- Cisco Secure Firewall Compatibility Guide
- Threat Defense Configuration Guide
- Cisco Smart Software Manager
- Security Cloud Control Documentation