Frequently Asked Questions

Frequently Asked Questions

Q. What are the new features supported on Secure Firewall migration tool release 4.0?

A. The following features are supported with release 4.0:

- Migration of FDM-managed device to a threat defense device managed by either the management center or the cloud-delivered Firewall Management Center.
- Migration of Equal Cost Multi-Path (ECMP) routes from ASA.
- Migration of Policy Based Routing (PBR) from ASA.
- Migration of Remote Access VPN custom attributes and VPN load balancing from ASA.

Q. What are the new features supported on Secure Firewall migration tool release 3.0.1?

A. The following features are supported with release 3.0.1:

- Migration of Enhanced Interior Gateway Routing Protocol (EIGRP) from ASA.
- Secure Firewall 3100 series is supported as a source or destination device for ASA migrations.

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

A. The following features are supported with release 3.0:

- Remote Access VPN migration
- Migration to Cloud-delivered Firewall Management Center

Q. What are the new features supported on Secure Firewall migration tool release 2.5.1?

A. The following features are supported with release 2.5.1:

- Dynamic Route objects

Frequently Asked Questions

- Border Gateway Protocol

Q. What are the new features supported on Secure Firewall migration tool release 2.5?
A. The following features are supported with release 2.5:

- ACL Optimization
- Wildcard mask

Q. What are the new features supported on Secure Firewall migration tool release 2.4?
A. The following ASA VPN configuration migration to threat defense:

- Crypto map (static/dynamic) based VPN from ASA
- Route-based (VTI) ASA VPN
- Certificate-based VPN migration from ASA

Q. What are the new features supported on Secure Firewall migration tool release 2.3.5?
A. The following features are supported with release 2.3.5:

- Virtual Tunnel Interface (VTI) and related configurations in Static routes, ACL.
- Route-based (VTI) VPN tunnels

Q. What are the new features supported on Secure Firewall migration tool release 2.3.4?
A. The following features are supported with release 2.3.4:

- VPN Objects
- Site-to-Site VPN Tunnels

Q. What are the source and target platforms that the Secure Firewall migration tool can migrate policy?
A. The Secure Firewall migration tool can migrate policies from supported ASA platform to threat defense platform. For more information, see Supported Source ASA Platforms.

Q. What are the tasks that you must perform in the Pre-Migration and Post-Migration Reports?
A. To perform the tasks as part of your plan for migrating from ASA to Firewall Threat Defense, see Sample Migrtion: ASA to Threat Defense 2100.

Q. What are the supported destination platforms versions?
A. You can use the Secure Firewall migration tool to migrate an ASA configuration to the standalone or container instance of the Firewall Threat Defense platforms for management center 6.2.3 or later. For more information on the list of supported devices, see Supported Target Threat Defense Platforms.

Q. What are the features the Secure Firewall migration tool supports for migration?
A. The Secure Firewall migration tool supports migration of L3/L4 ASA configuration to threat defense. It also allows enabling L7 features like IPS, file policy, and so on, during the migration process.

The Secure Firewall migration tool can fully migrate the following ASA configurations:

- Network objects and groups (except discontiguous masks)
- Service objects, except for those service objects configured for a source and destination

Note Though the Secure Firewall migration tool does not migrate extended service objects (configured for a source and destination), referenced ACL and NAT rules are migrated with full functionality.

- Service object groups, except for nested service object groups, VPN objects, and ASA crypto map VPN migration

Note Since nesting is not supported on the management center, the Secure Firewall migration tool expands the content of the referenced rules. The rules, however, are migrated with full functionality.

- IPv4 and IPv6 FQDN objects and groups
- IPv6 conversion support (Interface, Static Routes, Objects, ACL, and NAT)
- Access rules that are applied to interfaces in the inbound direction and global ACL
- Auto NAT, Manual NAT, and object NAT (conditional)
- Static routes, except for those configured with the track option which are partially migrated and ECMP routes which are not migrated
- Physical interfaces
- Subinterfaces
- Port channels
- Bridge groups (transparent mode only)
- Tunneling protocol-based access control policy rules (migrated as Prefilter tunnel rules)
- Category-based rule for CSM managed configurations
- IP SLA Monitor
- Object Group Search
- Time-based Objects
- VPN objects
- VTI interfaces
- Policy-based (Crypto Map) and Route-based (VTI) VPN tunnels
- Certificate-based VPN migration from ASA to threat defense
- Dynamic Route objects for EIGRP and BGP

- Remote Access VPN

Q. What are the new features supported on the Secure Firewall migration tool for Release 2.2?
A. The following features are supported with release 2.2:

- Object Group Search
- IP SLA Monitor
- Time-based Objects

Q. What are the new features supported on the Secure Firewall migration tool for Release 2.0?
A. The following features are supported with release 2.0:

- Destination Zone mapping for Access Rules
- Prefilter tunnel rules
- Category-based rules
- Policy Limit and Capacity Warning
- ASA 5505 and ASA-SM migration support

Q. Is there any dependency on management center to use the new features introduced in the Secure Firewall migration tool?
A. Yes. The following features are supported with target management center 6.5 and later:

- Migrate tunnel Rules as Prefilter
- Category-based rules
- ASA 5505 Migration

Note Requires management centerversion 6.5 and later to migrate to target threat defense FPR-1010 platform.

The following features are supported with target management center 6.6 and later:

- Object Group Search
- IP SLA Monitor
- Time-based Objects
- VPN Objects
- Site-to-Site VPN Tunnels

The following features are supported with target management center 6.7 and later:

- VTI interface and the related static routes.
- Route-based (VTI) Pre-Shared Key authentication type VPN configuration to management center.

- Create routed security zone, add VTI interfaces, and then define access control rules for the decrypted traffic control over VTI tunnel.

The following features are supported with target management center 7.1 and later:

- Dynamic Route objects
- BGP

The following features are supported with target management center 7.2 and later:

- Remote Access VPN
- EIGRP

Q. Can we migrate all the access rules in the source configuration to the Prefilter policy?

A. No. For migrations that are opted with **Migrate Tunnel rules as Prefilter**, the Secure Firewall migration tool identifies tunneling protocol-based access rules and migrates them as tunnel rules.

Q. What are the features the Secure Firewall migration tool does not migrate today?

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

- SGT-based access control policy rules
- SGT-based objects
- User-based access control policy rules
- NAT rules that are configured with the block allocation option
- Objects with unsupported ICMP type and code
- Tunneling protocol-based access control policy rules
- NAT rules that are configured with SCTP
- NAT rules that are configured with host ‘0.0.0.0’
- Tunneling protocol-based access control policy rules (supported from Secure Firewall migration tool 2.0 with target management center 6.5 and later)
- Dynamic Crypto map based VPN
- Certificate authentication based VPN configuration

For more information, see Guidelines and Limitations.

Q. What are the supported source devices and code version?

A. You can use the Secure Firewall migration tool to migrate the configuration from single or multi-context ASA platforms (software version 8.4 or later). For more information on the list of devices, see Supported Source ASA Platforms.

Q. Does the Secure Firewall migration tool support migration of multi-context ASA?

A. Yes. The Secure Firewall migration tool can handle migration of multi-context ASA. At any given point in time, one can migrate one context of the ASA (except for *System* context) to either threat defense container or native instances on the target management center.

Q. What is the support mechanism if there are migration errors?

A. The Secure Firewall migration tool is integrated with Cisco Success Network. If there are errors or issues, contact Cisco TAC. For troubleshooting, see Troubleshooting Migration Issues.

Q. How much time does the Secure Firewall migration tool take to successfully migrate a configuration?

A. The time that is taken during migration depends on numerous factors like latency on network, load on the management center, config size, number of objects, ACL, and so on. In internal testing, it was observed that a config file of 2.0 MB with 7000+ Access Control List, 7000+ NAT Translations, and 3000+ Network Objects takes around 6 minutes to successfully complete the migration.