

Cisco Secure Firewall 마이그레이션 툴 설명서 탐색하기

초판: 2020년 6월 8일

최종 변경: 2021년 7월 30일

Cisco Secure Firewall 마이그레이션 툴 설명서 탐색하기

Firewall 마이그레이션 툴 소개

Cisco Secure Firewall 마이그레이션 툴은 지원되는 ASA, FPS 포함 ASA, Check Point, PAN(Palo Alto Network) 및 Fortinet Firewall 컨피그레이션을 지원되는 threat defense 플랫폼으로 변환합니다. 지원되는 기능 및 정책의 마이그레이션을 자동화할 수 있지만 지원되지 않는 기능은 수동으로 구성해야 합니다.

Firewall 마이그레이션 툴 설명서 개요

Firewall 마이그레이션 툴 개요 - Firewall 마이그레이션 툴을 사용하여 ASA, ASA(FPS), CP(Check Point), PAN(Palo Alto Networks) 또는 Fortinet을 threat defense virtual로 마이그레이션하는 방법에 대한 정보는 최신 버전의 Firewall 마이그레이션 툴을 설명합니다. 최신 버전의 Firewall 마이그레이션 툴을 다운로드하려면 [Cisco.com](#)에서 **Firewall 마이그레이션 툴 다운로드**에 나온 지침을 따르십시오.

Firewall 마이그레이션 툴은 ASA, FPS 포함 ASA, Check Point, PAN, Fortinet 정보를 수집하고 구문 분석한 다음 마지막으로 management center에 푸시합니다. 구문 분석 단계에서 Firewall 마이그레이션 툴은 마이그레이션 전 보고서를 생성합니다. 이 문서에서는 Firewall 마이그레이션 툴 다운로드부터 마이그레이션 완료까지 Firewall 마이그레이션 툴에 대한 정보를 제공합니다. 또한 마이그레이션 문제를 해결하는 데 도움이 되는 문제 해결 팁도 제공합니다.

Firewall 마이그레이션 툴 소프트웨어 다운로드 페이지 - 소프트웨어 다운로드 페이지에서 최신 버전의 소프트웨어를 다운로드합니다. 자세한 내용을 보려면, [Cisco.com](#)에서 **Firewall 마이그레이션 툴 다운로드**를 참고하십시오.

Firepower 마이그레이션 툴 릴리즈 노트

Firewall 마이그레이션 툴 릴리즈 노트 - 이 문서에서는 중요 및 릴리즈별 정보를 제공합니다.

ASA Firewall을 Secure Firewall Management Center에서 관리하는 Secure Firewall Threat Defense로 마이그레이션

Firewall 마이그레이션 툴을 사용하여 지원되는 소스 구성을 Firewall 릴리스 6.2.3 이상에 대해 지원되는 threat defense 구성으로 마이그레이션할 수 있습니다.

ASA Firewall을 Management Center에서 관리하는 Threat Defense로 마이그레이션 — 이 문서에서는 지원되는 ASA 컨피그레이션을 지원되는 threat defense 플랫폼으로 변환하는 절차를 설명합니다. Firewall 마이그레이션 툴을 사용하면 지원되는 ASA 기능 및 정책의 마이그레이션을 자동화할 수 있습니다.

다음 문서는 threat defense로의 ASA 마이그레이션과 관련이 있습니다.

- [ASA에서 Threat Defense로 인증서 마이그레이션](#) - Cisco ASA에서 threat defense 디바이스로 ID 및 CA(Certificate Authority) 인증서를 마이그레이션하는 절차를 설명합니다.
- [인증서와 함께 IKEv1을 사용하여 ASA를 Threat Defense Site-to-Site VPN으로 마이그레이션](#) - 인증서(rsa-sig)를 인증 방법으로 사용하여 기존 Cisco ASA로부터 관리되는 threat defense로 사이트 대 사이트 IKEv1 VPN 터널을 마이그레이션하는 절차를 설명합니다.
- [인증서와 함께 IKEv2를 사용하여 ASA를 Threat Defense Site-to-Site VPN으로 마이그레이션](#) - 인증서(rsa-sig)를 인증 방법으로 사용하여 기존 ASA로부터 management center에서 관리하는 threat defense로 사이트 대 사이트 IKEv2 VPN 터널을 마이그레이션하는 절차를 설명합니다.
- [ASA를 FTD의 Threat Defense 유동 암호화 맵 기반 사이트 대 사이트 터널로 마이그레이션](#) - 사전 공유 키와 인증서를 인증 방법으로 사용하여 기존 ASA으로부터 management center에서 관리하는 threat defense로 유동 암호화 맵 기반 사이트 대 사이트 VPN 터널(IKEv1 또는 IKEv1 사용)을 마이그레이션하는 절차를 설명합니다.
- [사전 공유 키 인증과 함께 IKEv1을 사용하여 ASA를 Threat Defense Site-to-Site VPN으로 마이그레이션](#) - PSK(Pre-Shared Key)를 인증 방법으로 사용하여 기존 ASA으로부터 management center에서 관리하는 threat defense로 사이트 대 사이트 IKEv1 VPN 터널을 마이그레이션하는 절차를 설명합니다.
- [사전 공유 키 인증과 함께 IKEv2를 사용하여 ASA를 Threat Defense Site-to-Site VPN으로 마이그레이션](#) - PSK(Pre-Shared Key)를 인증 방법으로 사용하여 기존 ASA로부터 management center에서 관리하는 threat defense로 사이트 대 사이트 IKEv2 VPN 터널을 마이그레이션하는 절차를 설명합니다.
- [ASA를 Threat Defense 플랫폼 설정으로 마이그레이션](#) - ASA의 플랫폼 설정 컨피그레이션을 threat defense 디바이스로 마이그레이션하는 단계를 설명합니다.

FirePOWER Services(FPS) Firewall을 사용하는 ASA를 Management Center에서 관리하는 Secure Firewall Threat Defense로 마이그레이션

FirePOWER Services(FPS) Firewall을 사용하는 ASA를 Management Center에서 관리하는 Threat Defense로 마이그레이션 — 이 문서에서는 지원되는 FPS 포함 ASA 컨피그레이션을 지원되는 threat defense 플랫폼으로 변환하는 절차를 설명합니다. Firewall 마이그레이션 툴을 사용하면 지원되는 FPS 포함 ASA 기능 및 정책의 마이그레이션을 자동화할 수 있습니다.

ASA Firewall을 Cisco Defense Orchestrator에서 관리하는 Threat Defense로 마이그레이션

[ASA Firewall을 CDO에서 관리하는 Threat Defense로 마이그레이션](#) — 이 문서에서는 ASA를 threat defense 디바이스로 마이그레이션하는 절차를 설명합니다. CDO는 ASA에서 실행 중인 구성의 다음 요소를 threat defense 템플릿으로 마이그레이션하는 데 도움이 되는 마법사를 제공합니다.

Check Point Firewall을 Management Center에서 관리하는 Threat Defense로 마이그레이션

[Check Point Firewall을 Management Center에서 관리하는 Threat Defense로 마이그레이션](#) — 이 문서에서는 지원되는 Check Point 컨피그레이션을 지원되는 threat defense 플랫폼으로 변환하는 절차를 설명합니다. Firewall 마이그레이션 툴을 사용하면 지원되는 Check Point 기능 및 정책의 마이그레이션을 자동화할 수 있습니다.

Palo Alto Networks(PAN) Firewall을 Management Center에서 관리하는 Threat Defense로 마이그레이션

[Palo Alto Networks Firewall을 Management Center에서 관리하는 Threat Defense로 마이그레이션](#) — 이 문서에서는 지원되는 PAN 컨피그레이션을 지원되는 threat defense 플랫폼으로 변환하는 절차를 설명합니다. Firewall 마이그레이션 툴을 사용하면 지원되는 PAN 기능 및 정책의 마이그레이션을 자동화할 수 있습니다.

Fortinet Firewall을 Management Center에서 관리하는 Threat Defense로 마이그레이션

[FortiNet Firewall을 Management Center에서 관리하는 Threat Defense로 마이그레이션](#) — 이 문서에서는 지원되는 FortiNet 컨피그레이션을 지원되는 threat defense 플랫폼으로 변환하는 절차를 설명합니다. Firewall 마이그레이션 툴을 사용하면 지원되는 FortiNet 기능 및 정책의 마이그레이션을 자동화할 수 있습니다.

Firewall 마이그레이션 툴 호환성 가이드

[Firewall 마이그레이션 툴 호환성 가이드](#) - 이 문서에서는 Firewall 마이그레이션 툴 시스템 소프트웨어 및 하드웨어 호환성 및 요구 사항을 설명합니다.

Firewall 마이그레이션 툴 오류 메시지

[Firewall 마이그레이션 툴 오류 메시지](#) - 이 문서에서는 마이그레이션 중에 발생할 수 있는 오류에 대한 해결 방법 및 오류 메시지를 제공합니다.

Firewall 마이그레이션 툴 오픈 소스

[Firewall 마이그레이션 툴 오픈 소스 설명서](#) — 이 문서에는 마이그레이션 중에 사용된 오픈 소스 소프트웨어에 대한 라이선스 및 알림이 나열되어 있습니다.

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

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

The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on standards documentation, or language that is used by a referenced third-party product.

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)

© 2022 Cisco Systems, Inc. 모든 권리 보유.

번역에 관하여

Cisco는 일부 지역에서 본 콘텐츠의 현지 언어 번역을 제공할 수 있습니다. 이러한 번역은 정보 제공의 목적으로만 제공되며, 불일치가 있는 경우 본 콘텐츠의 영어 버전이 우선합니다.