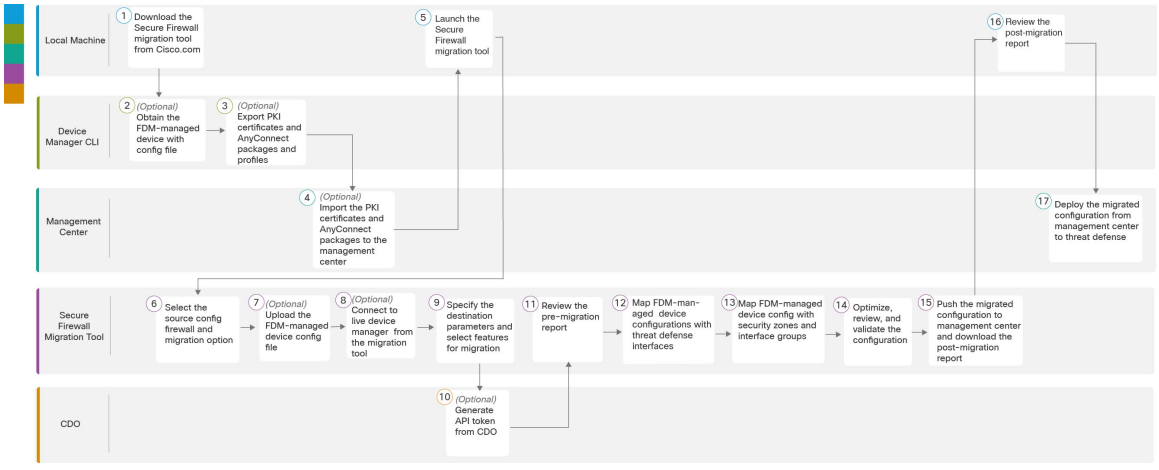
FDM 매니지드 디바이스-Threat Defense 워크플로우

엔드 투 엔드 절차

다음 순서도는 Secure Firewall 마이그레이션 툴을 사용하여 FDM 매니지드 디바이스를 Threat Defense로 마이그레이션하는 워크플로우를 보여줍니다.



	업무 환경	단계
1	로컬 컴퓨터	Cisco.com에서 Secure Firewall 마이그레이션 툴의 최신 버전을 다운로드합니다. 자세한 단계는 Cisco.com에서 Secure Firewall 마이그레이션 툴 다운로드를 참고하십시오.

	업무 환경	단계
2	Device Manager CLI	(선택 사항) FDM 매니지드 디바이스 구성 파일 가져오기: Device Manager CLI에서 FDM 매니지드 디바이스 구성 파일을 가져오려면 FDM 매니지드 디바이스 구성 파일 가져오기를 참고하십시오. Secure Firewall 마이그레이션 툴에서 FDM 매니지드 디바이스를 연결하려는 경우 3단계로 건너뜁니다.
3	Device Manager CLI	(선택 사항) PKI 인증서 및 AnyConnect 패키지와 프로파일 내보내기: 이 단계는 사이트 대 사이트 VPN 및 RA VPN 기능을 FDM 매니지드 디바이스에서 Threat Defense로 마이그레이션하려는 경우에만 필요합니다. Device Manager CLI에서 PKI 인증서를 내보내려면 Device Manager에서 PKI 인증서 내보내기 및 Firewall Management Center로 가져오기를 참고하십시오. Device Manager CLI에서 AnyConnect 패키지 및 프로파일을 내보내려면 AnyConnect 패키지 및 프로파일 검색를 참고하십시오. 사이트 대 사이트 VPN 및 RA VPN을 마이그레이션할 계획이 없는 경우 7단계로 건너뜁니다.
4	Management Center	(선택 사항) PKI 인증서 및 AnyConnect 패키지를 Management Center로 가져오기: PKI 인증서를 Management Center로 가져오려면 Device Manager에서 PKI 인증서 내보내기 및 Firewall Management Center로 가져오기 및 AnyConnect 패키지 및 프로파일 검색를 참고하십시오.
5	로컬 컴퓨터	로컬 컴퓨터에서 Secure Firewall 마이그레이션 툴을 실행합니다(Secure Firewall 마이그레이션 툴 실행 참조).
6	Secure Firewall 마이그레이션 툴	소스 구성 방화벽 및 마이그레이션 옵션을 선택하려면 소스 구성 및 Device Manager 마이그레이션 옵션 선택을 참고하십시오.
7	Secure Firewall 마이그레이션 툴	(선택 사항) Device Manager CLI에서 가져온 FDM 매니지드 디바이스 구성 파일을 업로드합니다(FDM 구성 번들 업로드 참조). 라이브 FDM 매니지드 디바이스에 연결하려는 경우 8단계로 건너뜁니다.
8	Secure Firewall 마이그레이션 툴	Secure Firewall 마이그레이션 툴에서 라이브 Device Manager에 직접 연결할 수 있습니다. 자세한 내용은 Secure Firewall 마이그레이션 툴에서 FDM 매니지드 디바이스에 연결을 참고하십시오.
9	Secure Firewall 마이그레이션 툴	이 단계에서 마이그레이션의 대상 매개변수를 지정할 수 있습니다. 자세한 단계는 Secure Firewall 마이그레이션 툴에 대한 대상 매개변수 지정을 참고하십시오.
10	CDO	(선택 사항) 이 단계는 선택 사항이며, 클라우드 사용 Firewall Management Center를 대상 Management Center로 선택한 경우에만 필요합니다. 자세한 단계는 Secure Firewall 마이그레이션 툴에 대한 대상 매개변수 지정를 참고하십시오.
11	Secure Firewall 마이그레이션 툴	마이그레이션 전 보고서를 다운로드한 위치로 이동하여 보고서를 검토합니다. 자세한 단계는 마이그레이션 전 보고서 검토를 참고하십시오.

	업무 환경	단계
12	Secure Firewall 마이그레이션 툴	Secure Firewall 마이그레이션 툴을 사용하면 FDM 매니지드 디바이스 구성을 Threat Defense 인터페이스와 매핑할 수 있습니다. 자세한 단계는 FDM 매니지드 디바이스 구성과 Secure Firewall Device Manager Threat Defense 인터페이스 매핑을 참고하십시오.
13	Secure Firewall 마이그레이션 툴	FDM 매니지드 디바이스 구성이 올바르게 마이그레이션되도록 하려면 FDM 매니지드 디바이스 인터페이스를 적절한 Threat Defense 인터페이스 개체, 보안 영역 및 인터페이스 그룹에 매핑합니다. 자세한 단계는 FDM 매니지드 디바이스 인터페이스를 보안 영역에 매핑을 참고하십시오.
14	Secure Firewall 마이그레이션 툴	구성을 최적화하고 신중하게 검토하여 구성이 올바른지 확인하고 Threat Defense 디바이스를 구성하는 방법과 일치하는지 확인합니다. 자세한 단계는 마이그레이션할 컨피그레이션 최적화, 검토 및 검증을 참고하십시오.
15	Secure Firewall 마이그레이션 툴	마이그레이션 프로세스의 이 단계에서는 마이그레이션된 구성을 Management Center로 전송하며, 마이그레이션 후 보고서를 다운로드할 수 있습니다. 자세한 단계는 마이그레이션된 컨피그레이션을 Management Center에 푸시를 참고하십시오.
16	로컬 컴퓨터	마이그레이션 후 보고서를 다운로드한 위치로 이동하여 보고서를 검토합니다. 자세한 단계는 마이그레이션 후 보고서 검토 및 마이그레이션 완료를 참고하십시오.
17	Management Center	Management Center에서 Threat Defense로 마이그레이션된 구성을 구축합니다. 자세한 단계는 마이그레이션 후 보고서 검토 및 마이그레이션 완료를 참고하십시오.

마이그레이션 사전 요건

FDM 매니지드 디바이스 구성을 마이그레이션하기 전에 다음 활동을 수행합니다.

Cisco.com에서 Secure Firewall 마이그레이션 툴 다운로드

시작하기 전에

Cisco.com에 인터넷으로 연결되는 Windows 10 64비트 또는 macOS 10.13 이상 버전 시스템이 있어야 합니다.

단계 **1** 컴퓨터에서 Secure Firewall 마이그레이션 툴용 폴더를 생성합니다.

이 폴더에는 다른 파일을 저장하지 않는 것이 좋습니다. Secure Firewall 마이그레이션 툴을 실행하면 로그, 리소스 및 기타 모든 파일이 이 폴더에 저장됩니다.

참고 Secure Firewall 마이그레이션 툴의 최신 버전을 다운로드할 때마다 새 폴더를 생성하고 기존 폴더를 사용하지 않아야 합니다.

단계 **2** https://software.cisco.com/download/home/286306503/type으로 이동하여 **Firewall** 마이그레이션 툴을 클릭합니다.

위 링크를 클릭하면 Firewall NGFW Virtual 아래의 Secure Firewall 마이그레이션 툴로 이동합니다. 위협 방어 디바이스 다운로드 영역에서 Secure Firewall 마이그레이션 툴을 다운로드할 수도 있습니다.

단계 **3** 생성한 폴더에 최신 버전의 Secure Firewall 마이그레이션 툴을 다운로드합니다.

Windows 또는 macOS 시스템용 Secure Firewall 마이그레이션 툴의 해당 실행 파일을 다운로드합니다.

FDM 매니지드 디바이스 구성 파일 가져오기

다음 방법 중 하나를 사용하여 FDM 매니지드 디바이스 구성 파일을 가져올 수 있습니다.

- FDM 매니지드 디바이스 구성 파일 내보내기, 4 페이지
- Secure Firewall 마이그레이션 툴에서 FDM 매니지드 디바이스에 연결, 15 페이지

FDM 매니지드 디바이스 구성 파일 내보내기

이 작업은 FDM 매니지드 디바이스 구성 파일을 수동으로 업로드하려는 경우에만 필요합니다. Threat Defense API를 사용하여 Device Manager의 구성 파일을 내보낼 수 있습니다. 구성을 내보내면 시스템이 ZIP 파일을 만듭니다. ZIP 파일을 로컬 워크스테이션에 다운로드할 수 있습니다. 이 구성 자체는 JSON 형식 텍스트 파일에서 특성-값 쌍을 사용하여 정의된 개체로 표시됩니다.

내보내기를 수행할 때 내보내기 파일에 포함할 구성을 지정해야 합니다. 전체 내보내기에는 내보내기 zip 파일의 모든 구성이 포함됩니다.

내보내기 zip 파일에는 다음 항목이 포함될 수 있습니다.

- 구성된 각 개체를 정의하는 특성-값 쌍. 구성 가능한 모든 항목은 Device Manager에서 "개체"라고 부르는 항목이 아니라 개체로서 모델링됩니다.
- 원격 액세스 VPN, AnyConnect 패키지 및 기타 참조된 모든 파일(예: 클라이언트 프로파일 XML 파일, DAP XML 파일, Hostscan 패키지).
- 사용자 지정 파일 정책을 구성한 경우 참조되는 정리 목록 또는 사용자 지정 탐지 목록.

단계 **1** 내보내기용 JSON 개체 본문을 생성합니다.

예제:

JSON 개체의 예는 다음과 같습니다.

```
  "diskFileName": "string",
  "encryptionKey": "**********",
  "doNotEncrypt": false,
  "configExportType": "FULL_EXPORT",
  "deployedObjectsOnly": true,
  "entityIds": [
    "string"
  ],
  "jobName": "string",
  "type": "scheduleconfigexport"
}
```

속성은 다음과 같습니다.

- **diskFileName** - (선택 사항) 내보내기 zip 파일의 이름입니다. 이름을 지정하지 않으면 시스템이 기본적으로 이름을 생성합니다. 이름을 지정하는 경우에도 시스템에서 고유성을 보장하기 위해 이름에 문자를 추가할 수 있습니다. 이름의 최대 길이는 60자입니다.
- **encryptionKey** - zip 파일의 암호화 키입니다. 파일을 암호화하지 않으려면 이 필드를 건너뛰고 대신 **doNotEncrypt: true**를 지정합니다. 키를 지정한 경우 로컬 컴퓨터에 다운로드한 후 키를 사용하여 zip 파일을 엽니다. 내보낸 구성 파일은 암호 키, 비밀번호 및 기타 민감한 데이터를 일반 텍스트로 표시합니다. 다른 방법으로는 가져올 수 없습니다. 이 경우 민감한 데이터를 보호하기 위해 암호화 키를 적용할 수 있습니다. 시스템에서 AES 256 암호화를 사용합니다.
- **doNotEncrypt** - (선택 사항) 내보내기 파일을 암호화할지(false), 암호화하지 않을지(true) 여부를 지정합니다. 기본값은 false입니다. 즉, 비어 있지 않은 암호화 키 속성을 지정해야 합니다. true를 지정하면 암호화 키 속성이 무시됩니다.
- **configExportType** - 다음 내보내기 유형 중 하나를 선택하여 구성 파일을 내보낼 수 있습니다.
  - FULL_EXPORT - 전체 구성을 내보내기 파일에 포함합니다. 이는 기본 옵션이며 마이그레이션에 선택해야 합니다**.**
- **deployedObjectsOnly** - (선택 사항) 구축된 경우에만 내보내기 파일에 개체를 포함할지 여부입니다. 기본값은 false입니다. 이는 모든 보류 중인 변경 사항이 내보내기에 포함되었음을 의미합니다. 보류 중인 변경 사항을 제외하려면 true를 지정합니다.
- **entityIds** - 시작점 개체 집합이 있는 ID가 쉼표로 구분된 목록으로, [대괄호]로 묶여 있습니다. 이 목록은 PARTIAL_EXPORT 작업에 필요합니다. 이 목록의 각 항목은 UUID 값 또는 "id=uuid-value", "type=object-type", "name=object-name"과 같은 속성-값 쌍이 일치하는 패턴일 수 있습니다. 예를 들어 "type=networkobject"입니다.
  - type은 리프 엔터티(예: 네트워크 개체)이거나 리프 유형 집합의 별칭일 수 있습니다. 몇 가지 일반적인 유형의 별칭으로는 네트워크(NetworkObject 및 NetworkObjectGroup), 포트(모든 TCP/UDP/ICMP 포트, 프로토콜 및 그룹 유형), url(URL 개체 및 그룹), ikepolicy(IKE V1/V2 정책), ikeproposal(Ike V1/V2 제안), identitysource(모든 ID 소스), 인증서(모든 인증서 유형), 개체(Device Manager에서 Objects(개체) 페이지에 나열되는 모든 개체/그룹 유형), 인터페이스(모든 네트워크 인터페이스, s2svpn(모든 사이트 대 사이트 VPN 관련 유형), ravpn(모든 RA VPN 관련 유형), vpn(s2svpn 및 ravpn 둘 다)이 있습니다.
  - 이러한 모든 개체와 해당하는 발신 참조 하위 항목은 PARTIAL_EXPORT 출력 파일에 포함됩니다. 내보낼 수 없는 모든 개체는 ID를 지정한 경우에도 출력에서 제외됩니다. 적절한 리소스 유형에 대해 GET 메서드를 사용하여 대상 개체의 UUID, 유형 또는 이름을 가져옵니다.

예를 들어, 모든 네트워크 개체와 함께 myaccessrule이라는 액세스 규칙 및 UUID로 식별되는 개체 2개를 내보내려면 다음과 같이 지정하면 됩니다.

```
"entityIds": [
   "type=networkobject",
   "id=bab3e3cd-8c70-11e9-930a-1f12ee87d473",
   "name=myaccessrule",
   "acc2e3cd-8c70-11e9-930a-1f12ee87b286"
   ]",
```

- **jobName** - (선택 사항) 내보내기 작업의 이름을 지정하면 작업 상태를 검색할 때 더 쉽게 찾을 수 있습니다.
- **type** - 작업 유형이며, 항상 **scheduleconfigexport**입니다.

단계 **2** 개체를 게시합니다.

예제**:**

curl 명령은 다음과 같이 표시됩니다.

```
  curl -X POST --header 'Content-Type: application/json' --header 'Accept: application/json' -d '{ \
   "configExportType": "FULL_EXPORT", \
   "type": "scheduleconfigexport" \
}' 'https://10.89.5.38/api/fdm/latest/action/configexport'
```

단계 **3** 응답을 확인합니다.

응답 코드 200이 표시되어야 합니다. 최소 JSON 개체를 게시한 경우 성공적인 응답 본문은 다음과 같습니다.

```
{
  "version": null,
  "scheduleType": "IMMEDIATE",
  "user": "admin",
  "forceOperation": false,
  "jobHistoryUuid": "c7a8ba61-629a-11e9-8b8d-0fcc3c9d6d0b",
  "ipAddress": "10.24.5.177",
  "diskFileName": "export-config-1",
  "encryptionKey": null,
  "doNotEncrypt": true
  "configExportType": "FULL_EXPORT",
  "deployedObjectsOnly": false,
  "entityIds": null,
  "jobName": "Config Export",
  "id": "c79be920-629a-11e9-8b8d-85231be77de0",
  "type": "scheduleconfigexport",
  "links": {
    "self": "https://10.89.5.38/api/fdm/latest
/action/configexport/c79be920-629a-11e9-8b8d-85231be77de0"
  }
}
```

단계 **4** 구성 내보내기의 상태를 확인합니다.

내보내기를 완료하는 데는 시간이 약간 걸립니다. 구성할 항목이 많을수록 작업을 수행하는 데 더 많은 시간이 필요합니다. 작업 상태를 확인하여 파일 다운로드를 시도하기 전에 작업이 완료되었는지 확인합니다.

상태를 검색하는 가장 간단한 방법은 **GET /jobs/configexportstatus**를 사용하는 것입니다. 예를 들어 curl 명령은 다음과 같이 표시됩니다.

```
curl -X GET --header 'Accept: application/json'
'https://10.89.5.38/api/fdm/latest/jobs/configexportstatus'
```

성공적으로 완료된 작업은 다음 상태를 표시합니다.

```
{
  "version": "hdy62yf5xp3vf",
  "jobName": "Config Export",
  "jobDescription": null,
  "user": "admin",
  "startDateTime": "2019-04-19 13:14:54Z",
  "endDateTime": "2019-04-19 13:14:56Z",
  "status": "SUCCESS",
  "statusMessage": "The configuration was exported successfully",
  "scheduleUuid": "1ef502ad-62a5-11e9-8b8d-074ebc750708",
  "diskFileName": "export-config-1.zip",
  "messages": [],
  "configExportType": "FULL_EXPORT",
  "deployedObjectsOnly": false,
  "entityIds": null,
  "id": "1f0aad8e-62a5-11e9-8b8d-bb1ebb4d1300",
  "type": "configexportjobstatus",
  "links": {
    "self": "https://10.89.5.38/api/fdm/latest
/jobs/configexportstatus/1f0aad8e-62a5-11e9-8b8d-bb1ebb4d1300"
  }
}
```

단계 **5** 내보내기 파일을 다운로드합니다.

내보내기 작업이 완료되면 내보내기 파일이 시스템 디스크에 기록되며, 이 파일을 구성 파일이라고 합니다. **GET /action/downloadconfigfile/{objId}**를 사용하여 이 내보내기 파일을 로컬 시스템에 다운로드할 수 있습니다.

사용 가능한 파일 목록을 가져오려면 GET /action/configfiles 메서드를 사용합니다.

```
curl -X GET --header 'Accept: application/json'
'https://10.89.5.38/api/fdm/latest/action/configfiles'
```

응답에는 항목 목록이 표시되며 각 항목은 구성 파일입니다. 예를 들어, 다음 목록에는 2개의 파일이 표시됩니다. 모든 파일의 ID는 기본값이며, 모범 사례로 ID를 무시하고 대신 diskFileName을 사용할 수 있습니다.

```
{
  "items": [
    {
      "diskFileName": "export-config-2.zip",
      "dateModified": "2019-04-19 13:32:28Z",
      "sizeBytes": 10182,
      "id": "default",
      "type": "configimportexportfileinfo",
      "links": {
        "self": "https://10.89.5.38/api/fdm/latest/action/configfiles/default"
      }
    },
    {
      "diskFileName": "export-config-1.zip",
      "dateModified": "2019-04-19 13:14:56Z",
      "sizeBytes": 10083,
      "id": "default",
      "type": "configimportexportfileinfo",
      "links": {
        "self": "https://10.89.5.38/api/fdm/latest/action/configfiles/default"
      }
    }
  ],
```

diskFileName을 개체 ID로 사용하여 파일을 다운로드합니다.

```
curl -X GET --header 'Accept: application/octet-stream'
'https://10.89.5.38/api/fdm/latest/action/downloadconfigfile/export-config-2.zip'
```

파일은 기본 다운로드 폴더에 다운로드됩니다. API Explorer에서 GET 메서드를 실행하고 브라우저가 다운로드 위치를 확인하도록 구성된 경우 파일을 저장하라는 메시지가 표시됩니다.

참고 다운로드에 성공하면 반환 코드 200이 생성되며 응답 본문이 없습니다.

Device Manager에서 PKI 인증서 내보내기 및 Firewall Management Center로 가져오기

Secure Firewall 마이그레이션 툴은 Management Center로의 인증서 기반 VPN 마이그레이션을 지원합니다.

가져온 FDM 매니지드 디바이스 구성 번들에는 키와 함께 인증서 페이로드가 포함되어 있습니다. 이는 Management Center에서 가져올 수 있습니다.

대상 Management Center에서 마이그레이션 전 활동의 일부로 트러스트 포인트 또는 VPN 인증서를 PKI 개체로 수동으로 마이그레이션합니다. 이 활동은 Secure Firewall 마이그레이션 툴을 사용하여 마이그레이션을 시작하기 전에 수행해야 합니다.

단계 **1** 구성 번들에서 인증서 페이로드(-----BEGIN CERTIFICATE----- 및 -----END CERTIFICATE----- 사이의 값) 및 키(-----BEGIN RSA PRIVATE KEY----- 및 -----END RSA PRIVATE KEY----- 사이의 값)를 복사합니다.

예제:

```
   "type":"identitywrapper",
   "action":"CREATE",
   "data":{
      "version":"girr7veykdjvx",
      "name":"RA_VPN_Cert",
      "cert":"-----BEGIN
[redacted]
 CERTIFICATE-----",
      "privateKey":"-----BEGIN RSA PRIVATE
[redacted]
 RSA PRIVATE KEY-----",
      "issuerCommonName":"mojave-rsa-root-2048-sha384.cisco.com, CN =
mojave-rsa-root-2048-sha384.cisco.com",
      "issuerCountry":"US",
      "issuerOrganization":"Cisco",
      "subjectCommonName":"fdm-ra-vpn-cert.cisco.com, CN = 172.16.10.50",
      "subjectCountry":"US",
     "subjectDistinguishedName":" C = US, O = Cisco, CN = fdm-ra-vpn-cert.cisco.com, CN = 172.16.10.50",

      "subjectOrganization":"Cisco",
      "validityStartDate":"Jan  1 12:00:00 2012 GMT",
      "validityEndDate":"Sep  1 12:00:00 2034 GMT",
      "isSystemDefined":false,
      "keyType":"RSA",
      "keySize":2048,
      "allowWeakCert":false,
      "signatureHashType":"SHA1",
```

```
        "weakCertificate":true,
        "id":"9d0a8efb-01fa-11ed-8d7b-1f4809c453ac",
        "type":"internalcertificate"
    }
}
```

단계 **2** PKI 인증서를 Management Center(**Object Management(**개체 관리**)** > **PKI Objects(PKI** 개체**)**)로 가져옵니다

자세한 내용은 Firewall Management Center 구성 가이드를 참고하십시오.

수동으로 생성한 PKI 개체는 이제 **VPN Tunnels(VPN** 터널**)** 섹션의 **Review and Validate(**검토 및 검증**)** 페이지에 있는 Secure Firewall 마이그레이션 툴에서 사용할 수 있습니다.

AnyConnect 패키지 및 프로파일 검색

시작하기 전에

AnyConnect 프로파일은 선택 사항이며, Management Center 또는 Secure Firewall 마이그레이션 툴을 통해 업로드할 수 있습니다.

- Management Center의 원격 액세스 VPN에는 하나 이상의 AnyConnect 패키지가 필요합니다.
- 구성이 Hostscan 및 외부 브라우저 패키지로 구성된 경우 이러한 패키지를 업로드해야 합니다.
- 모든 패키지는 마이그레이션 전 활동의 일부로 Management Center에 추가해야 합니다.
- Dap.xml 및 Data.xml은 Secure Firewall 마이그레이션 툴을 통해 추가해야 합니다.

다운로드할 Device Manager에서 사용 가능한 패키지를 확인합니다.

단계 **1** 다운로드할 Device Manager에서 사용 가능한 패키지를 확인합니다.

GET /object/anyconnectpackagefiles API를 사용하여 디바이스의 패키지를 볼 수 있습니다.

```
curl -X GET --header 'Accept: application/json' '
 https://10.89.5.38/api/fdm/v6/object/anyconnectpackagefiles'
```

이 명령은 Device Manager에서 사용 가능한 AnyConnect 패키지를 검색합니다.

```
{
  "items": [
    {
      "version": "gx5yk7xkdsosu",
      "name": "anyconnect-win-4.10.02086-webdeploy-k9.pkg",
      "md5Checksum": "63e4a86fc7c68d7769b6a1b2976ffa73",
      "description": null,
      "diskFileName": "12f0988e-01fb-11ed-8d7b-07ecdd54c7bf.pkg",
      "platformType": "WINDOWS",
      "id": "133f2dbf-01fb-11ed-8d7b-89d64ab04e18",
      "type": "anyconnectpackagefile",
      "links": {
        "self": "
https://10.89.5.38/api/fdm/v6/object/anyconnectpackagefiles/133f2dbf-01fb-11ed-8d7b-89d64ab04e18"
      }
```

```
    }
  ],
}
```

응답의 diskFilename은 AnyConnect 패키지를 다운로드하는 데 사용됩니다.

단계 **2** AnyConnect 패키지를 다운로드합니다.

GET /action/downloaddiskfile/{objId}를 사용하여 AnyConnect 패키지를 로컬 워크스테이션에 다운로드할 수 있습니다. 사용되는 개체 ID는 AnyConnect 패키지 응답의 diskFileName(12f0988e-01fb-11ed-8d7b-07ecdd54c7bf.pkg)입니다.

```
curl -X GET --header 'Accept: application/octet-stream'
' https://10.89.5.38/api/fdm/v6/action/downloaddiskfile/12f0988e-01fb-11ed-8d7b-07ecdd54c7bf.pkg'
```

단계 **3** Device Manager에서 사용 가능한 AnyConnect 프로파일을 확인합니다.

참고 AnyConnect 프로파일은 Secure Firewall 마이그레이션 툴에 의해 Device Manager에서 자동으로 검색됩니다. 이 단계는 AnyConnect 프로파일을 수동으로 업로드하려는 경우에만 필요합니다.

GET /object/anyconnectclientprofiles를 사용하여 Device Manager에서 사용 가능한 프로파일을 확인할 수 있습니다.

```
curl -X GET --header 'Accept: application/json'
'https://10.196.155.3:12272/api/fdm/v6/object/anyconnectclientprofiles'
```

다음 응답이 표시됩니다.

```
  "items": [

    {
      "version": "jqtwzirf36qke",
      "name": "AnyConnect_VPN_Profile",
      "md5Checksum": "e4ba581f84daec6f24c209f9f7f9e1fb",
      "description": null,
      "diskFileName": "1629395a-0384-11ed-8d7b-ab1a2a5ad583.xml",
      "anyConnectModuleType": "ANY_CONNECT_CLIENT_PROFILE",
      "id": "1754c10b-0384-11ed-8d7b-6b8e36ae1285",
      "type": "anyconnectclientprofile",
    }
  ]
}
```

응답의 diskFilename은 AnyConnect 프로파일을 다운로드하는 데 사용됩니다.

단계 **4** AnyConnect 프로파일을 다운로드합니다.

GET /action/downloaddiskfile/{objId}를 사용하여 AnyConnect 패키지를 로컬 워크스테이션에 다운로드할 수 있습니다. 사용되는 objId는 AnyConnect 프로파일 응답의 diskFileName(1629395a-0384-11ed-8d7b-ab1a2a5ad583.xml)입니다.

```
curl -X GET --header 'Accept: application/octet-stream'
'https://10.196.155.3:12272/api/fdm/v6/action/downloaddiskfile/1629395a-0384-11ed-8d7b-ab1a2a5ad583.xml'
```

단계 **5** 다운로드한 패키지를 Management Center(**ObjectManagement >)** > **VPN** > **AnyConnect File(AnyConnect** 파일**)**로 가져옵니다.

1. Dap.xml 및 Data.xml을 **Review and Validate(**검토 및 검증**)** > **Remote Access VPN(**원격 액세스 **VPN)** > **AnyConnect File(AnyConnect** 파일**)** 섹션을 통해 Secure Firewall 마이그레이션 툴에서 Management Center로 업로드해야 합니다.
2. AnyConnect 프로파일은 Management Center에 직접 업로드하거나 **Review and Validate(**검토 및 검증**)** > **Remote Access VPN(**원격 액세스 **VPN)** > **AnyConnect File(AnyConnect** 파일**)**의 Secure Firewall 마이그레이션 툴을 통해 업로드할 수 있습니다.

수동으로 업로드한 파일을 이제 Secure Firewall 마이그레이션 툴에서 사용할 수 있습니다.

마이그레이션 실행

Secure Firewall 마이그레이션 툴 실행

참고 Secure Firewall 마이그레이션 툴을 실행하면 별도의 창에 콘솔이 열립니다. 마이그레이션을 진행하는 동안 Secure Firewall 마이그레이션 툴의 현재 단계 진행률이 콘솔에 표시됩니다. 화면에 콘솔이 표시되지 않으면 Secure Firewall 마이그레이션 툴의 뒤에 있을 가능성이 높습니다.

시작하기 전에

- Cisco.com에서 Secure Firewall 마이그레이션 툴 다운로드
- 마이그레이션에 지원되는 대상 Management Center 섹션의 요구 사항을 검토하고 확인합니다.
- Secure Firewall 마이그레이션 툴을 실행하려면 컴퓨터에 최신 버전의 Google Chrome 브라우저가 있어야 합니다. Google Chrome을 기본 브라우저로 설정하는 방법에 대한 자세한 내용은 Chrome을 기본 웹 브라우저로 설정을 참고하십시오.
- 대규모 컨피그레이션 파일을 마이그레이션하려는 경우 마이그레이션 푸시 중에 시스템이 절전 모드로 전환되지 않도록 절전 설정을 구성합니다.

단계 **1** 컴퓨터에서 Secure Firewall 마이그레이션 툴을 다운로드한 폴더로 이동합니다.

단계 **2** 다음 중 하나를 수행합니다.

- Windows 시스템에서 Secure Firewall 마이그레이션 툴 실행 파일을 더블 클릭하여 Google Chrome 브라우저에서 실행합니다.

  프롬프트가 표시되면 **Yes(**예**)**를 클릭하여 Secure Firewall 마이그레이션 툴에서 시스템을 변경할 수 있도록 허용합니다.

Secure Firewall 마이그레이션 툴은 Log(로그) 및 Resources(리소스) 폴더를 포함하여 해당 파일이 있는 폴더에 모든 관련 파일을 생성하고 저장합니다.

- Mac에서 Secure Firewall 마이그레이션 툴*.command 파일을 원하는 폴더로 이동하고, 터미널 애플리케이션을 실행하고, Secure Firewall 마이그레이션 툴이 설치된 폴더로 이동한 후 다음 명령을 실행합니다.

```
# chmod 750 Firewall_Migration_Tool-version_number.command
# ./Firewall_Migration_Tool-version_number.command
```

Secure Firewall 마이그레이션 툴은 Log(로그) 및 Resources(리소스) 폴더를 포함하여 해당 파일이 있는 폴더에 모든 관련 파일을 생성하고 저장합니다.

팁 Secure Firewall 마이그레이션 툴을 열려고 하면 확인된 개발자가 Secure Firewall 마이그레이션 툴을 Apple에 등록하지 않았으므로 경고 대화 상자가 표시됩니다. 확인되지 않은 개발자로부터 애플리케이션을 여는 방법에 대한 자세한 내용은 확인되지 않은 개발자의 앱 열기를 참고하십시오.

참고 MAC 터미널 압축 방법을 사용합니다.

단계 **3** Cisco와 텔레메트리 정보를 공유하려는 경우 **End User License Agreement(**엔드 유저 라이선스 계약**)** 페이지에서 **I agree to share data with Cisco Success Network(Cisco Success Network**와 데이터 공유 동의**)**를 클릭하고, 그렇지 않은 경우 **I'll do later(**나중에**)**를 클릭합니다.

Cisco Success Network로 통계를 전송하는 데 동의하면 Cisco.com 계정을 사용하여 로그인하라는 메시지가 표시됩니다. Cisco Success Network로 통계를 보내지 않도록 선택하는 경우 로컬 자격 증명을 사용하여 Secure Firewall 마이그레이션 툴에 로그인합니다.

단계 **4** **Reset Password(**비밀번호 재설정**)** 페이지에서 이전 비밀번호와 새 비밀번호를 입력하고 확인을 위해 새 비밀번호를 다시 입력합니다.

새 비밀번호는 8자 이상이어야 하며 대문자, 소문자, 숫자 및 특수 문자를 포함해야 합니다.

단계 **5** **Reset(**재설정**)**을 클릭합니다.

단계 **6** 새 비밀번호로 로그인합니다.

참고 비밀번호를 잊어버린 경우 <*migration_tool_folder*>에서 기존의 모든 데이터를 삭제하고 Secure Firewall 마이그레이션 툴을 다시 설치합니다.

단계 **7** 마이그레이션 전 체크리스트를 검토하고 나열된 모든 항목을 완료했는지 확인합니다.

체크리스트에서 하나 이상의 항목을 완료하지 않은 경우, 완료할 때까지 계속하지 마십시오.

단계 **8** **New Migration(**새 마이그레이션**)**을 클릭합니다.

단계 **9** Secure Firewall 마이그레이션 툴의 최신 버전을 실행하고 있는지 확실하지 않은 경우 **Software Update Check(**소프트웨어 업데이트 확인**)** 화면에서 Cisco.com을 통해 버전을 확인하는 링크를 클릭합니다.

단계 **10** **Proceed(**진행**)**를 클릭합니다.

다음에 수행할 작업

다음 단계로 진행할 수 있습니다.

• FDM 매니지드 디바이스 구성을 컴퓨터로 내보낸 경우 FDM 구성 번들 업로드로 진행합니다.

소스 구성 및 Device Manager 마이그레이션 옵션 선택

단계 1 드롭다운 목록에서 **Source Firewall Vendor(**소스 방화벽 벤더**)**를 선택하고 **Start Migration(**마이그레이션 시작**)**을 클릭합니다.

단계 2 FDM 매니지드 디바이스를 마이그레이션할 마이그레이션 옵션을 선택합니다.

다음 옵션을 사용할 수 있습니다.

- **Firepower Device Manager** 마이그레이션**(**공유 구성만 해당**)**

  이 옵션을 사용하면 Device Manager에서 대상 Management Center로 공유 구성을 마이그레이션할 수 있습니다. 이 옵션은 미리 구성된 마이그레이션에 사용해야 합니다. 그래야 공유 구성이 처음에 마이그레이션되고 나중에 디바이스 구성이 마이그레이션될 수 있습니다. 이 활용 사례에는 다운타임이 없습니다.

- **Firepower Device Manager** 마이그레이션**(**디바이스 및 공유 구성 포함**)**

  이 옵션을 사용하면 공유 및 디바이스 구성을 대상 Management Center로 마이그레이션할 수 있습니다. 이 마이그레이션의 일부로 소스 Threat Defense가 Device Manager에서 Management Center로 이동합니다. 마이그레이션이 성공적으로 완료되면 Management Center는 계속해서 Threat Defense 디바이스를 관리합니다. 따라서 이 활용 사례에서는 소스와 대상이 동일한 Threat Defense 디바이스입니다. Threat Defense 디바이스가 Management Center로 이동하므로 이 활용 사례에는 관련 다운타임이 있습니다.

  이 옵션을 사용하여 구성을 마이그레이션하려면 마이그레이션 전 활동의 일부로 다음을 수행합니다.

  1. Device Manager에 로그인하고 **Objects(**개체**)** 섹션으로 이동합니다.
  2. **Identity Sources(ID** 소스**)**를 클릭하고 **Preset filters(**사전 설정 필터**)**에서 **AD Realm(AD** 영역**)**을 선택합니다.
  3. **Actions(**작업**)** 아래에서 암호화 유형이 **LDAPS** 또는 **STARTTLS**인 특정 영역에 대해 **Edit(**수정**)** (✎) 아이콘을 클릭합니다.
  4. **Directory Server Configuration(**디렉터리 서버 구성**)**에서 서버 이름 옆에 있는 드롭다운 화살표를 클릭합니다.
  5. **Encryption(**암호화**)** 섹션에서 암호화 유형을 **NONE(**없음**)**으로 변경하고 **OK(**확인**)**를 클릭합니다.
  6. 변경 사항을 구축하고

  참고 구성이 Management Center로 마이그레이션되면 Management Center에서 AD 영역의 암호화 유형을 LDAPS 또는 STARTTLS로 되돌릴 수 있습니다. 자세한 단계는 마이그레이션 후 보고서 검토 및 마이그레이션 완료를 참고하십시오.

- **Firepower Device Manager(**디바이스 및 공유 구성 포함**)**를 **FTD** 디바이스**(**새 하드웨어**)**로 마이그레이션

이 옵션을 사용하면 FDM 매니지드 디바이스 구성을 대상 Management Center에 이미 등록된 Threat Defense로 마이그레이션할 수 있습니다. 소스 FDM 매니지드 디바이스의 구성이 대상 Management Center에 등록된 사용자가 선택한 대상 Threat Defense로 마이그레이션됩니다. 이 활용 사례에는 다운타임이 없습니다.

FDM 구성 번들 업로드

시작하기 전에

소스 Device Manager에서 구성 번들을 `.zip`으로 내보냅니다.

참고 수동 업로드는 아래의 두 옵션에 대해 지원됩니다.

- **Firepower Device Manager(**디바이스 및 공유 구성 포함**)**를 **FTD** 디바이스**(**새 하드웨어**)**로 마이그레이션
- **Firepower Device Manager** 마이그레이션**(**공유 구성만 해당**)**

단계 **1** **Extract FDM Information(FDM** 정보 추출**)** 화면의 **Manual Upload(**수동 업로드**)** 섹션에서 **Upload(**업로드**)**를 클릭하여 FDM 매니지드 구성 번들을 업로드합니다. 구성 번들이 암호화된 경우 Secure Firewall 마이그레이션 툴의 텍스트 상자에 키를 입력하여 번들을 해독합니다.

단계 **2** FDM 매니지드 디바이스 구성 파일이 있는 위치로 이동하여 **Open(**열기**)**을 클릭합니다.

Secure Firewall 마이그레이션 툴이 구성 번들을 업로드합니다. 대규모 컨피그레이션 파일의 경우 이 단계는 시간이 더 오래 걸립니다. 콘솔에서는 구문 분석 중인 FDM 매니지드 디바이스 구성을 포함하여 진행 상황의 라인별 로그 보기를 제공합니다. 콘솔이 표시되지 않는 경우 Secure Firewall 마이그레이션 툴 뒤의 별도 창에서 콘솔을 찾을 수 있습니다.

단계 **3** **Start Parsing(**구문 분석 시작**)**을 클릭합니다.

Parsed Summary(구문 분석 요약**)** 섹션에 구문 분석 상태가 표시됩니다.

단계 **4** 업로드된 구성 파일에서 Secure Firewall 마이그레이션 툴이 감지하고 구문 분석한 요소에 대한 요약을 검토합니다.

단계 **5** **Next(**다음**)**를 클릭하여 대상 매개변수를 선택합니다.

다음에 수행할 작업

Secure Firewall 마이그레이션 툴에 대한 대상 매개변수 지정

Secure Firewall 마이그레이션 툴에서 FDM 매니지드 디바이스에 연결

시작하기 전에

Secure Firewall 마이그레이션 툴은 마이그레이션할 FDM 매니지드 디바이스에 연결하여 필요한 구성 정보를 추출할 수 있습니다. FDM 매니지드 디바이스에 대한 Live Connect는 세 가지 사용 사례 모두에서 지원됩니다.

- Secure Firewall 마이그레이션 툴을 다운로드하여 실행합니다.
- FDM 매니지드 디바이스에서 Management Center로의 마이그레이션에 대해 수행할 활용 사례를 선택합니다.
- 관리 IP 주소, Device Manager의 관리자 자격 증명을 가져옵니다.

단계 **1** **Extract FDM Information(FDM** 정보 추출**)** 화면의 **Connect to FDM(FDM**에 연결**)** 섹션에서 **Connect(**연결**)**를 클릭하여 마이그레이션할 FDM 매니지드 디바이스에 연결합니다.

단계 **2** **FDM Login(FDM** 로그인**)** 화면에서 다음 정보를 입력합니다.

1. **FDM IP Address/Hostname(FDM IP** 주소/호스트 이름**)** 필드에 FDM의 관리 IP 주소 또는 호스트 이름을 입력합니다. **Login(**로그인**)**을 클릭합니다.
2. **Username(**사용자 이름**)**, **Password(**비밀번호**)** 필드에 해당 관리자 로그인 자격 증명을 입력합니다.
3. **Login(**로그인**)**을 클릭합니다.

Secure Firewall 마이그레이션 툴이 FDM 매니지드 디바이스에 연결되면 마이그레이션을 진행하기 전에 FDM 매니지드 디바이스에서 일련의 컴플라이언스 확인이 수행됩니다. 이러한 확인은 사전 요건 및 모범 사례 섹션에서 다룹니다. 확인에 성공하면 마이그레이션이 다음 단계로 진행됩니다.

Secure Firewall 마이그레이션 툴이 FDM 매니지드 디바이스에 연결되고, 컴플라이언스 확인이 성공하면 툴이 구성 정보 추출을 시작합니다. 추출이 성공적으로 완료되면 구문 분석된 요약 페이지가 표시됩니다.

Parsed Summary(구문 분석 요약**)** 섹션에 구문 분석 상태가 표시됩니다.

단계 **3** Secure Firewall 마이그레이션 툴이 FDM 매니지드 디바이스에서 검색하여 구문 분석한 요소의 요약을 검토합니다.

단계 **4** **Next(**다음**)**를 클릭하여 대상 매개변수를 선택합니다.

다음에 수행할 작업

Secure Firewall 마이그레이션 툴에 대한 대상 매개변수 지정

Secure Firewall 마이그레이션 툴에 대한 대상 매개변수 지정

시작하기 전에

CDO에서 호스팅되는 마이그레이션 툴의 클라우드 버전을 사용하는 경우 단계 3로 건너뜁니다.

- 온프레미스 Firewall Management Center용 management center의 IP 주소를 가져옵니다.
- (선택 사항) 선택한 플로우가 management center에 대해 **Firepower Device Manager(**디바이스 및 공유 구성 포함**)**를 **FTD** 디바이스**(**새 하드웨어**)**로 마이그레이션인 경우 Management Center에 대상 Threat Defense 디바이스를 추가합니다. Firewall Management Center에 디바이스 추가 참고
- **Review and Validate(**검토 및 검증**)** 페이지에서 ACL에 IPS 또는 파일 정책을 적용해야 하는 경우 마이그레이션 전에 management center에서 정책을 생성하는 것이 매우 권장됩니다. Secure Firewall 마이그레이션 툴이 연결된 management center에서 정책을 가져오므로 동일한 정책을 사용합니다. 새 정책을 생성하고 여러 액세스 제어 목록에 할당하면 성능이 저하될 수 있으며 푸시가 실패할 수도 있습니다.

단계 **1** **Select Target(**대상 선택**)** 화면의 **Firewall Management(**방화벽 관리**)** 섹션에서 다음을 수행합니다.

- 온프레미스 Firewall Management Center로 마이그레이션하려면 다음을 수행합니다.

a) **On-Prem FMC(**온프레미스 **FMC)** 라디오 버튼을 클릭합니다.
b) Management Center의 IP 주소 또는 FQDN(정규화된 도메인 이름)을 입력합니다.
c) **Domain(**도메인**)** 드롭다운 목록에서 마이그레이션할 도메인을 선택합니다.

Firepower Device Manager(디바이스 및 공유 구성 포함**)**를 **FTD** 디바이스**(**새 하드웨어**)**로 마이그레이션을 고른 경우 선택한 도메인에서 사용 가능한 Threat Defense 디바이스로만 마이그레이션할 수 있습니다.

d) **Connect(**연결**)**를 클릭하고 **2**단계로 진행합니다.

- 클라우드 사용 Firewall Management Center로 마이그레이션하려면 다음을 수행합니다.

a) **Cloud** 사용 **FMC** 라디오 버튼을 클릭합니다.
b) 지역을 선택하고 CDO API 토큰을 붙여넣습니다. API 토큰을 생성합니다. CDO에서 다음 단계를 수행합니다.
   1. CDO 포털에 로그인합니다.
   2. **Settings(**설정**)** > **General Settings(**일반 설정**)**로 이동하여 API 토큰을 복사합니다.
c) **Connect(**연결**)**를 클릭하고 **2**단계로 진행합니다.

단계 **2** **Firewall Management Center Login(Firewall Management Center** 로그인**)** 대화 상자에서 Secure Firewall 마이그레이션 툴 전용 계정의 사용자 이름과 비밀번호를 입력하고 **Login(**로그인**)**을 클릭합니다.

Secure Firewall 마이그레이션 툴이 management center에 로그인하여 해당 management center에서 관리되는 위협 방어 디바이스 목록을 검색합니다. 콘솔에서 이 단계의 진행 상황을 볼 수 있습니다.

단계 **3** **Proceed(**진행**)**를 클릭합니다.

Firepower Device Manager(디바이스 및 공유 구성 포함**)**를 **FTD** 디바이스**(**새 하드웨어**)**로 마이그레이션을 고른 경우 선택한 도메인에서 사용 가능한 Threat Defense 디바이스로만 마이그레이션할 수 있습니다.

Firepower Device Manager 마이그레이션**(**공유 구성만 해당**)**을 선택한 경우

Management Center의 Threat Defense 섹션은 이 워크플로에서 채워지지 않으며, 공유 정책(액세스 제어 목록, NAT 및 개체)만 FMC에 푸시됩니다. Management Center에 푸시해야 하는 공유 정책을 포함하거나 건너뛸 수 있습니다.

Firepower Device Manager 마이그레이션**(**디바이스 및 공유 구성 포함**)**을 선택한 경우

Management Center로 이동되는 Threat Defense는 Device Manager가 관리하는 디바이스와 동일합니다. 이 경우 Management Center의 Threat Defense 부분이 채워지지 않습니다.

단계 **4** **Choose Threat Defense(**위협 방어 선택**)** 섹션에서 다음 중 하나를 수행합니다.

- **Select Firewall Threat Defense Device(Firewall Threat Defense** 디바이스 선택**)** 드롭다운 목록을 클릭하고 FDM 매니지드 디바이스 구성을 마이그레이션할 디바이스를 선택합니다.

  선택한 management center 도메인의 디바이스가 **IP Address(IP** 주소**)** 및 **Name(**이름**)**별로 나열됩니다.

  참고 지원되는 대상 Threat Defense 플랫폼이 Management Center 버전 6.5 이상을 사용하는 Firewall 1010인 경우에만 FDM 5505 마이그레이션 지원은 공유 정책에 적용되며 디바이스별 정책에는 적용되지 않습니다. Threat Defense 없이 진행하면 Secure Firewall 마이그레이션 툴이 Threat Defense에 구성 또는 정책을 푸시하지 않습니다. 따라서 Threat Defense 디바이스별 구성인 인터페이스 및 경로, 사이트 대 사이트 VPN은 마이그레이션되지 않습니다. 그러나 NAT, ACL 및 포트 개체와 같은 지원되는 다른 모든 컨피그레이션(공유 정책 및 개체)은 마이그레이션됩니다. 원격 액세스 VPN은 공유 정책이며 Threat Defense 없이도 마이그레이션할 수 있습니다.

- 컨피그레이션을 management center로 마이그레이션하려면 **Proceed without Threat Defense(Threat Defense** 없이 진행**)**를 클릭합니다.

  위협 방어 없이 진행하면 Secure Firewall 마이그레이션 툴이 위협 방어에 구성 또는 정책을 푸시하지 않습니다. 따라서 위협 방어 디바이스별 컨피그레이션인 인터페이스 및 경로, 사이트 대 사이트 VPN은 마이그레이션되지 않습니다. 그러나 NAT, ACL 및 포트 개체와 같은 지원되는 다른 모든 컨피그레이션(공유 정책 및 개체)은 마이그레이션됩니다. 원격 액세스 VPN은 공유 정책이며 Threat Defense 없이도 마이그레이션할 수 있습니다.

단계 **5** **Proceed(**진행**)**를 클릭합니다.

마이그레이션하는 대상에 따라 Secure Firewall 마이그레이션 툴에서 마이그레이션할 기능을 선택할 수 있습니다.

단계 **6** **Select Features(**기능 선택**)** 섹션을 클릭하여 대상으로 마이그레이션할 기능을 검토하고 선택합니다.

- 대상 위협 방어 디바이스로 마이그레이션하는 경우 Secure Firewall 마이그레이션 툴이 **Device Configuration(**디바이스 구성**)** 및 **Shared Configuration(**공유 구성**)** 섹션의 FDM 매니지드 디바이스 구성에서 마이그레이션에 사용할 수 있는 기능을 자동으로 선택합니다. 요구 사항에 따라 기본 선택 항목을 추가로 수정할 수 있습니다.
- management center로 마이그레이션하는 경우 Secure Firewall 마이그레이션 툴이 **Shared Configuration(**공유 구성**)** 섹션의 FDM 매니지드 디바이스 구성에서 마이그레이션에 사용할 수 있는 기능을 자동으로 선택합니다. 요구 사항에 따라 기본 선택 항목을 추가로 수정할 수 있습니다.

참고 **Firepower Device Manager** 마이그레이션**(**공유 구성만 해당**)**을 선택한 경우 **Device Configuration(**디바이스 구성**)** 섹션을 사용할 수 없습니다.

- Secure Firewall 마이그레이션 툴은 마이그레이션 중에 다음과 같은 액세스 제어 기능을 지원합니다.
  - 대상 보안 영역 채우기 - 마이그레이션 중에 ACL에 대한 대상 영역의 매핑을 활성화합니다.

    경로 조회 논리는 정적 경로와 연결된 경로로 제한되며, PBR과 유동 경로, NAT는 고려되지 않습니다. 인터페이스 네트워크 컨피그레이션은 연결된 경로 정보를 도출하는 데 사용됩니다.

    소스 및 대상 네트워크 개체 그룹의 특성에 따라 이 작업으로 인해 규칙이 급증할 수 있습니다.

  -
    - 심층 검사 맞춤화 - 캡슐화된 트래픽에 대해 가능하며 단축경로(Fastpath)를 지정하여 성능을 높일 수 있습니다.
    - 성능 향상 - 조기에 처리하는 것이 유리한 그 밖의 연결도 단축경로를 지정하거나 차단할 수 있습니다.

    Secure Firewall 마이그레이션 툴은 소스 구성에서 캡슐화된 터널 트래픽 규칙을 식별하고 이를 사전 필터 터널 규칙으로 마이그레이션합니다. 사전 필터 정책에서 마이그레이션된 터널 규칙을 확인할 수 있습니다. 사전 필터 정책은 management center에서 마이그레이션된 액세스 제어 정책과 연결됩니다.

    사전 필터 터널 규칙으로 마이그레이션되는 프로토콜은 다음과 같습니다.

    - GRE(47)
    - IPv4 캡슐화(4)
    - IPv6 캡슐화(41)
    - Teredo 터널링(UDP:3544)

    참고 사전 필터 옵션을 선택하지 않으면 모든 터널링된 트래픽 규칙이 지원되지 않는 규칙으로 마이그레이션됩니다.

    FDM 매니지드 디바이스 구성의 ACL 터널 규칙(GRE 및 IPnIP)은 현재 기본적으로 양방향으로 마이그레이션됩니다. 이제 액세스 제어 상태 옵션에서 대상의 규칙 방향을 양방향 또는 단방향으로 지정할 수 있습니다.

- Secure Firewall 마이그레이션 툴은 VPN 터널 마이그레이션을 위해 다음 인터페이스 및 개체를 지원합니다.
  - 정책 기반(암호화 맵) - 대상 management center 및 위협 방어가 버전 6.6 이상인 경우.
  - 경로 기반(VTI) - 대상 management center 및 위협 방어가 버전 6.7 이상인 경우.

- Secure Firewall 마이그레이션 툴은 대상 Management Center가 7.2 이상인 경우 원격 액세스 VPN의 마이그레이션을 지원합니다. 원격 액세스 VPN은 Threat Defense 없이도 마이그레이션할 수 있는 공유 정책입니다. Threat Defense를 사용하여 마이그레이션을 선택한 경우 Threat Defense 버전은 7.0 이상이어야 합니다.
- (선택 사항) **Optimization(**최적화**)** 섹션에서 **Migrate only referenced objects(**참조된 개체만 마이그레이션**)**를 선택하여 액세스 제어 정책 및 NAT 정책에서 참조되는 개체만 마이그레이션합니다.

참고 이 옵션을 선택하면 FDM 매니지드 디바이스 구성에서 참조되지 않는 개체는 마이그레이션되지 않습니다. 이렇게 하면 마이그레이션 시간이 최적화되고 컨피그레이션에서 사용되지 않는 개체가 제거됩니다.

- (선택 사항) **Optimization(최적화)** 섹션에서 위협 방어의 액세스 정책을 기준으로 최적의 메모리 사용률을 위한 **Object group search(개체 그룹 검색)**를 선택합니다.

단계 **7** **Proceed(진행)**를 클릭합니다.

단계 **8** **Rule Conversion/ Process Config(규칙 변환/프로세스 컨피그레이션)** 섹션에서 **Start Conversion(변환 시작)**을 클릭하여 변환을 시작합니다.

단계 **9** Secure Firewall 마이그레이션 툴에서 변환한 요소의 요약을 검토합니다.

컨피그레이션 파일이 성공적으로 업로드되고 구문 분석되었는지 확인하려면 마이그레이션을 계속하기 전에 **Pre-Migration Report(마이그레이션 전 보고서)**를 다운로드하여 확인하십시오.

단계 **10** **Download Report(보고서 다운로드)**를 클릭하고 **Pre-Migration Report(마이그레이션 전 보고서)**를 저장합니다.

Pre-Migration Report(마이그레이션 전 보고서)의 사본도 Secure Firewall 마이그레이션 툴과 동일한 위치의 `Resources(리소스)` 폴더에 저장됩니다.

마이그레이션 전 보고서 검토

마이그레이션 중에 마이그레이션 전 보고서를 다운로드하지 못한 경우 다음 링크를 사용하여 다운로드하십시오.

마이그레이션 전 보고서 다운로드 엔드포인트 - http://localhost:8888/api/downloads/pre_migration_summary_html_format

참고 Secure Firewall 마이그레이션 툴이 실행 중일 때만 보고서를 다운로드할 수 있습니다.

단계 **1** **Pre-Migration Report(마이그레이션 전 보고서)**를 다운로드한 위치로 이동합니다.

Pre-Migration Report(마이그레이션 전 보고서)의 사본도 Secure Firewall 마이그레이션 툴과 동일한 위치의 `Resources(리소스)` 폴더에 저장됩니다.

단계 **2** **Pre-Migration Report(마이그레이션 전 보고서)**를 열고 내용을 신중하게 검토하여 마이그레이션의 실패를 일으킬 수 있는 문제를 파악합니다.

Pre-Migration Report(마이그레이션 전 보고서)에는 다음 정보가 포함됩니다.

- **Overall Summary(전체 요약)** - FDM 매니지드 디바이스 구성 정보를 추출하거나 라이브 FDM 매니지드 디바이스 구성에 연결하는 데 사용되는 방법입니다.

  위협 방어로 성공적으로 마이그레이션할 수 있는 지원되는 FDM 매니지드 디바이스 구성 요소 및 마이그레이션을 위해 선택한 특정 기능의 요약입니다.

라이브 FDM 매니지드 디바이스에 연결하는 동안에는 요약에 적중 횟수 정보(FDM 매니지드 디바이스 규칙이 적용된 횟수 및 타임스탬프 정보)가 포함됩니다.

- **Configuration Lines with Errors(**오류가 있는 구성 라인**)** - Secure Firewall 마이그레이션 툴이 구문 분석할 수 없으므로, 마이그레이션할 수 없는 구성 요소에 대한 세부 정보입니다. 계속 진행하기 전에 구성에서 이러한 오류를 해결하고 새 구성 파일을 내보낸 다음 Secure Firewall 마이그레이션 툴에 새 구성 파일을 업로드합니다.
- **Partially Supported Configuration(**부분적으로 지원되는 구성**)** - 부분적으로만 마이그레이션할 수 있는 FDM 매니지드 디바이스 구성 요소에 대한 세부 정보입니다. 이러한 컨피그레이션 요소에는 고급 옵션이 있는 규칙 및 개체가 포함되는데, 이 경우 고급 옵션 없이 규칙 또는 개체를 마이그레이션할 수 있습니다. 이러한 라인을 검토하고 management center에서 고급 옵션이 지원되는지 확인한 다음, 지원되는 경우 Secure Firewall 마이그레이션 툴을 사용하여 마이그레이션을 완료한 후 해당 옵션을 수동으로 구성하도록 계획합니다.
- **Unsupported Configuration(**지원되지 않는 구성**)** - Secure Firewall 마이그레이션 툴이 해당 기능의 마이그레이션을 지원하지 않으므로 마이그레이션할 수 없는 FDM 매니지드 디바이스 구성 요소에 대한 세부 정보입니다. 이러한 라인을 검토하고 management center에서 각 기능이 지원되는지 확인한 다음, 지원되는 경우 Secure Firewall 마이그레이션 툴을 사용하여 마이그레이션을 완료한 후 해당 기능을 수동으로 구성하도록 계획합니다.
- **Ignored Configuration(**무시된 구성**)** - management center 또는 Secure Firewall 마이그레이션 툴에서 지원되지 않기 때문에 무시되는 FDM 매니지드 디바이스 구성 요소의 세부 정보입니다. Secure Firewall 마이그레이션 툴은 이러한 라인을 구문 분석하지 않습니다. 이러한 라인을 검토하고 management center에서 각 기능이 지원되는지 확인한 다음, 지원되는 경우 해당 기능을 수동으로 구성하도록 계획합니다.

management center 및 위협 방어에서 지원되는 기능에 대한 자세한 내용은 Management Center 컨피그레이션 가이드를 참고하십시오.

단계 **3** **Pre-Migration Report(**마이그레이션 전 보고서**)**에서 시정 조치를 권장하는 경우, 계속하기 전에 인터페이스에서 해당 시정 조치를 완료하고 FDM 매니지드 디바이스 구성 파일을 다시 내보낸 후 업데이트된 구성 파일을 업로드하십시오.

단계 **4** FDM 매니지드 디바이스 구성 파일이 성공적으로 업로드되고 구문 분석된 후 Secure Firewall 마이그레이션 툴로 돌아가 **Next(**다음**)**를 클릭하여 마이그레이션을 계속합니다.

다음에 수행할 작업

FDM 매니지드 디바이스 구성과 Secure Firewall Device Manager Threat Defense 인터페이스 매핑

FDM 매니지드 디바이스 구성과 Secure Firewall Device Manager Threat Defense 인터페이스 매핑

위협 방어 디바이스에는 FDM 매니지드 디바이스 구성에 사용되는 것과 같거나 더 많은 수의 물리적 및 포트 채널 인터페이스가 있어야 합니다. 이러한 인터페이스가 두 디바이스에서 동일한 이름을 가질 필요는 없습니다. 인터페이스 매핑 방법을 선택할 수 있습니다.

Map Threat Defense Interface(Threat Defense 인터페이스 매핑**)** 화면에서 Secure Firewall 마이그레이션 툴로 위협 방어 디바이스의 인터페이스 목록을 검색합니다. 기본적으로 Secure Firewall 마이그레

이션 툴은 인터페이스 ID에 따라 FDM 매니지드 디바이스의 인터페이스와 위협 방어 디바이스를 매핑합니다. 예를 들어, FDM 매니지드 디바이스 인터페이스의 '관리 전용' 인터페이스는 위협 방어 디바이스의 '관리 전용' 인터페이스에 자동으로 매핑되며 이를 변경할 수 없습니다.

위협 방어 인터페이스에 대한 FDM 매니지드 디바이스 인터페이스 매핑은 위협 방어 디바이스 유형에 따라 달라집니다.

- 대상 위협 방어가 네이티브 유형인 경우:
  - 위협 방어에서 같거나 더 많은 수의 FDM 매니지드 디바이스 인터페이스 또는 PC(Port Channel) 데이터 인터페이스(FDM 매니지드 디바이스 구성의 관리 전용 및 하위 인터페이스 제외)를 사용해야 합니다. 이 수가 더 적은 경우 대상 위협 방어에 필요한 인터페이스 유형을 추가합니다.
  - 하위 인터페이스는 물리적 인터페이스 또는 포트 채널 매핑을 기반으로 Secure Firewall 마이그레이션 툴에서 생성됩니다.
- 대상 위협 방어가 컨테이너 유형인 경우:
  - 위협 방어에서 같거나 더 많은 수의 FDM 매니지드 디바이스 인터페이스, 물리적 하위 인터페이스, 포트 채널 또는 포트 채널 하위 인터페이스(FDM 매니지드 디바이스 구성의 관리 전용 인터페이스 제외)를 사용해야 합니다. 이 수가 더 적은 경우 대상 위협 방어에 필요한 인터페이스 유형을 추가합니다. 예를 들어, 대상 위협 방어의 물리적 인터페이스 및 물리적 하위 인터페이스 수가 FDM 매니지드 디바이스 보다 100개 적을 경우 대상 위협 방어에서 추가 물리적 인터페이스 또는 물리적 하위 인터페이스를 생성할 수 있습니다.
  - 하위 인터페이스는 Secure Firewall 마이그레이션 툴로 생성되지 않습니다. 물리적 인터페이스, 포트 채널 또는 하위 인터페이스 간의 인터페이스 매핑만 허용됩니다.

시작하기 전에

management center에 연결하고 대상을 위협 방어로 선택했는지 확인합니다. 자세한 내용은 Secure Firewall 마이그레이션 툴에 대한 대상 매개변수 지정, 16 페이지를 참고하십시오.

참고 **Firepower Device Manager** 마이그레이션(공유 구성만 해당)을 사용하여 마이그레이션하는 경우에는 이 단계를 적용할 수 없습니다.

이 단계는 **Firepower Device Manager** 마이그레이션(디바이스 및 공유 구성 포함)에 대한 정보 제공용 단계입니다.

단계 **1** 인터페이스 매핑을 변경하려면 **Threat Defense Interface Name(Firepower Threat Defense** 인터페이스 이름**)**의 드롭다운 목록을 클릭하고 해당 인터페이스에 매핑할 인터페이스를 선택합니다.

관리 인터페이스의 매핑은 변경할 수 없습니다. 위협 방어 인터페이스가 FDM 매니지드 디바이스 인터페이스에 이미 할당된 경우 드롭다운 목록에서 해당 인터페이스를 선택할 수 없습니다. 할당된 모든 인터페이스는 회색으로 표시되며 사용할 수 없습니다.

하위 인터페이스는 매핑할 필요가 없습니다. Secure Firewall 마이그레이션 툴은 FDM 매니지드 디바이스 구성의 모든 하위 인터페이스에 대해 위협 방어 디바이스의 하위 인터페이스를 매핑합니다.

단계 **2** 각 FDM 매니지드 디바이스 인터페이스를 위협 방어 인터페이스에 매핑했으면 **Next(**다음**)**를 클릭합니다.

FDM 매니지드 디바이스 인터페이스를 보안 영역에 매핑

참고 FDM 매니지드 디바이스 구성에 액세스 목록 및 NAT 규칙이 포함되어 있지 않거나 이러한 정책을 마이그레이션하지 않도록 선택한 경우에는 이 단계를 건너뛰고 로 진행할 수 있습니다.마이그레이션할 컨피그레이션 최적화, 검토 및 검증, 23 페이지

FDM 매니지드 디바이스 구성이 올바르게 마이그레이션되도록 하려면 FDM 매니지드 디바이스 인터페이스를 적절한 위협 방어 인터페이스 개체, 보안 영역에 매핑합니다. FDM 매니지드 디바이스 구성에서 액세스 제어 정책 및 NAT 정책은 인터페이스 이름(nameif)을 사용합니다. management center에서 이러한 정책은 인터페이스 개체를 사용합니다. 또한 management center 정책은 인터페이스 개체를 다음과 같이 그룹화합니다.

- 보안 영역 — 하나의 인터페이스가 하나의 보안 영역에만 속할 수 있습니다.
- 인터페이스 그룹 — 하나의 인터페이스가 여러 인터페이스 그룹에 속할 수 있습니다.

Secure Firewall 마이그레이션 툴을 사용하면 보안 영역 및 인터페이스 그룹이 있는 인터페이스를 일대일로 매핑할 수 있습니다. 보안 영역 또는 인터페이스 그룹이 인터페이스에 매핑된 경우 management center에서 허용하더라도 다른 인터페이스에 매핑될 수 없습니다. management center의 보안 영역 및 인터페이스 그룹에 대한 자세한 내용은 인터페이스 개체: 인터페이스 그룹 및 보안 영역을 참고하십시오.

단계 **1** **Map Security Zones and Interface Groups(**보안 영역 및 인터페이스 그룹 매핑**)** 화면에서 사용 가능한 인터페이스, 보안 영역 및 인터페이스 그룹을 검토합니다.

단계 **2** management center에 존재하는, 즉 FDM 매니지드 디바이스 구성 파일에서 보안 영역 유형 개체로 사용 가능하고 드롭다운 목록에서 사용 가능한 보안 영역 및 인터페이스 그룹에 인터페이스를 매핑하려면 다음과 같이 합니다.

a) **Security Zones(**보안 영역**)** 열에서 해당 인터페이스의 보안 영역을 선택합니다.
b) **Interface Groups(**인터페이스 그룹**)** 열에서 해당 인터페이스의 인터페이스 그룹을 선택합니다.

단계 **3** 보안 영역 및 인터페이스 그룹을 수동으로 매핑하거나 자동으로 생성할 수 있습니다.

단계 **4** 보안 영역 및 인터페이스 그룹을 수동으로 매핑하려면 다음과 같이 합니다.

a) **Add SZ & IG(SZ** 및 **IG** 추가**)**를 클릭합니다.
b) **Add SZ & IG(SZ** 및 **IG** 추가**)** 대화 상자에서 **Add(**추가**)**를 클릭하여 새 보안 영역 또는 인터페이스 그룹을 추가합니다.
c) **Security Zone(**보안 영역**)** 열에 보안 영역 이름을 입력합니다. 허용되는 최대 문자 수는 48자입니다. 마찬가지로 인터페이스 그룹을 추가할 수 있습니다.

d) **Close(**닫기**)**를 클릭합니다.

자동 생성을 통해 보안 영역 및 인터페이스 그룹을 매핑하려면 다음과 같이 합니다.

a) **Auto-Create(**자동 생성**)**를 클릭합니다.
b) **Auto-Create(**자동 생성**)** 대화 상자에서 **Interface Groups(**인터페이스 그룹**)** 및 **Zone Mapping(**영역 매핑**)** 중 하나 또는 둘 다를 선택합니다.
c) **Auto-Create(**자동 생성**)**를 클릭합니다.

Secure Firewall 마이그레이션 툴은 이러한 보안 영역에 FDM 매니지드 디바이스 인터페이스와 같은 이름(예: **outside(**외부**)** 또는 **inside(**내부**)**)을 지정하고 이름 뒤에 "(A)"를 표시하여 Secure Firewall 마이그레이션 툴에서 생성되었음을 나타냅니다. 인터페이스 그룹에는 **outside_ig** 또는 **inside_ig**와 같은 `_ig` 접미사가 추가됩니다. 또한 보안 영역 및 인터페이스 그룹은 FDM 매니지드 디바이스 인터페이스와 동일한 모드를 사용합니다. 예를 들어 FDM 매니지드 디바이스 논리적 인터페이스가 L3 모드인 경우 인터페이스에 대해 생성된 보안 영역 및 인터페이스 그룹도 L3 모드입니다.

단계 **5** 모든 인터페이스를 적절한 보안 영역 및 인터페이스 그룹에 매핑했으면 **Next(**다음**)**를 클릭합니다.

마이그레이션할 컨피그레이션 최적화, 검토 및 검증

FDM 매니지드 디바이스 구성의 경우 구성은 다양한 방법으로 검증되며, 선택한 마이그레이션 플로우에 따라 달라집니다. 다양한 옵션에 대한 구성 검증은 다음과 같습니다.

- **Firepower Device Manager(**디바이스 및 공유 구성 포함**)**를 **FTD** 디바이스**(**새 하드웨어**)**로 마이그레이션 - 단일 플로우에서 디바이스 및 공유 구성을 모두 검토하고 검증합니다.
- **Firepower Device Manager** 마이그레이션**(**공유 구성만 해당**)** - 공유 구성만 검토하고 검증합니다.
- **Firepower Device Manager** 마이그레이션**(**디바이스 및 공유 구성 포함**)** - 공유 및 디바이스 구성을 별도의 플로우에서 검증합니다.

공유된 컨피그레이션 최적화, 검토 및 검증

마이그레이션된 FDM 구성을 Management Center로 푸시하기 전에 구성을 최적화하고 신중하게 검토하여 해당 구성이 올바르며 위협 방 디바이스 구성 방법과 일치하는지 확인하십시오. 깜박이는 탭은 다음 작업 과정을 수행해야 함을 나타냅니다.

참고 **Optimize, Review and Validate Configuration(**구성 최적화**,** 검토 및 검증**)** 화면에서 Secure Firewall 마이그레이션 툴을 닫으면 진행 상황이 저장되고 나중에 마이그레이션을 재개할 수 있습니다. 이 화면 전에 Secure Firewall 마이그레이션 툴을 닫으면 진행 상황이 저장되지 않습니다. 구문 분석 후 오류가 발생한 경우 Secure Firewall 마이그레이션 툴을 다시 실행하면 **Interface Mapping(**인터페이스 매핑**)** 화면에서 재개됩니다.

여기서 Secure Firewall 마이그레이션 툴은 management center에 이미 있는 IPS(침입 방지 시스템) 정책 및 파일 정책을 가져와 마이그레이션 중인 액세스 제어 규칙에 연결할 수 있도록 합니다.

파일 정책은 네트워크에 대한 지능형 악성코드 차단 및 파일 제어를 수행하기 위해 시스템에서 전체 액세스 제어 구성의 일부로 사용하는 구성 집합입니다. 이 연결은 시스템이 액세스 제어 규칙의 조건에 일치하는 트래픽에 파일을 통과시키기 전에 먼저 파일을 검사하도록 합니다.

마찬가지로 트래픽이 대상으로 들어가기 전 시스템의 최후의 방어선으로 IPS 정책을 사용할 수 있습니다. 침입 정책은 보안 위반 확인을 위해 시스템이 인라인 배포에서 트래픽을 검사하는 방식을 제어하며, 악성 트래픽을 차단하거나 변경할 수 있습니다. 시스템이 트래픽 평가를 위해 침입 정책을 사용할 때마다, 연결된 변수 집합을 사용합니다. 집합 내 대부분의 변수는 소스 및 대상 IP 주소와 포트 확인을 위해 침입 규칙에서 일반적으로 사용되는 값을 나타냅니다. 규칙 삭제, 동적 규칙 상태의 IP 주소를 나타내려면 침입 정책 내 변수를 사용할 수도 있습니다.

탭에서 특정 컨피그레이션 항목을 검색하려면 열 맨 위의 필드에 항목 이름을 입력합니다. 검색어와 일치하는 항목만 표시하도록 테이블 행이 필터링됩니다.

Optimize, Review and Validate Configuration(컨피그레이션 최적화**,** 검토 및 검증**)** 화면에서 Secure Firewall 마이그레이션 툴을 닫으면 진행 상황이 저장되고 나중에 마이그레이션을 재개할 수 있습니다. 이 화면 전에 닫으면 진행 상황이 저장되지 않습니다. 구문 분석 후 오류가 발생한 경우 Secure Firewall 마이그레이션 툴을 다시 실행하면 **Interface Mapping(**인터페이스 매핑**)** 화면에서 재개됩니다.

Secure Firewall 마이그레이션 툴 **ACL** 최적화 개요

현재 Secure Firewall 마이그레이션 툴은 네트워크 기능에 영향을 주지 않고 방화벽 규칙 베이스에서 최적화(비활성화 또는 삭제)할 수 있는 ACL을 식별하고 분리하기 위한 지원을 제공합니다.

ACL 최적화는 다음 ACL 유형을 지원합니다.

- 중복 ACL - 두 ACL에 동일한 컨피그레이션 및 규칙 집합이 있는 경우 기본이 아닌 ACL을 제거해도 네트워크에 영향을 주지 않습니다. 예를 들어, 액세스 거부에 대해 정의된 규칙 없이 동일한 네트워크에서 FTP 및 IP 트래픽을 허용하는 두 규칙이 있는 경우 첫 번째 규칙을 삭제할 수 있습니다.
- 섀도우 ACL - 첫 번째 ACL은 두 번째 ACL의 컨피그레이션을 완전히 섀도잉합니다. 두 규칙에 유사한 트래픽이 있는 경우, 두 번째 규칙은 액세스 목록의 뒷부분에 나타나므로 어떤 트래픽에도 적용되지 않습니다. 두 규칙이 트래픽에 대해 서로 다른 작업을 지정하는 경우, 섀도잉된 규칙을 이동하거나 규칙 중 하나를 편집하여 필요한 정책을 구현할 수 있습니다. 예를 들어 기본 규칙은 IP 트래픽을 거부할 수 있으며, 섀도잉된 규칙은 지정된 소스 또는 대상에 대한 FTP 트래픽을 허용할 수 있습니다.

Secure Firewall 마이그레이션 툴은 ACL 최적화를 위한 규칙을 비교하는 동안 다음 매개변수를 사용합니다.

참고 최적화는 FDM 매니지드 디바이스 ACP 규칙 작업에만 사용할 수 있습니다.

- 비활성화된 ACL은 최적화 프로세스 중에 고려되지 않습니다.

- 소스 ACL은 해당 ACE(인라인 값)로 확장된 후 다음 매개변수에 대해 비교됩니다.
  - 소스 및 대상 영역
  - 소스 및 대상 네트워크
  - 소스 및 대상 포트

개체 최적화

마이그레이션 프로세스 중에 개체 최적화를 위해 다음 개체가 고려됩니다.

- 참조되지 않은 개체 - 마이그레이션을 시작할 때 참조되지 않은 개체를 마이그레이션하지 않도록 선택할 수 있습니다.
- 중복 개체 - 개체가 이미 management center에 있는 경우 중복 개체를 생성하는 대신 정책이 재사용됩니다.

단계 **1** (선택 사항) 화면에서 **Optimize ACL(ACL** 최적화**)**을 클릭하여 최적화 코드를 실행하고 다음을 수행합니다.

a) 식별된 ACL 최적화 규칙을 다운로드하려면 **Download(**다운로드**)**를 클릭합니다.

b) 규칙을 선택하고 **Actions(**작업**)** > **Migrate as disabled(**비활성화된 항목으로 마이그레이션**)** 또는 **Do not migration(**마이그레이션하지 않음**)**을 선택하고 작업 중 하나를 적용합니다.

c) **Save(**저장**)**를 클릭합니다.
마이그레이션 작업이 **Do not migrate(**마이그레이션하지 않음**)**에서 **disabled(**비활성화됨**)**로 또는 그 반대로 변경됩니다.

다음 옵션을 사용하여 규칙의 대량 선택을 수행할 수 있습니다.

- Migrate(마이그레이션) - 기본 상태로 마이그레이션합니다.
- Do not Migrate(마이그레이션 안 함) - ACL 마이그레이션을 무시합니다.
- Migrate as disabled(비활성화된 상태로 마이그레이션) - ***State(***상태***)*** 필드가 ***Disable(***비활성화***)***로 설정된 ACL을 마이그레이션합니다.
- Migrate as enabled(활성화된 상태로 마이그레이션) - ***State(***상태***)*** 필드가 ***Enable(***활성화***)***로 설정된 ACL을 마이그레이션합니다.

단계 **2** 최적화,**Review and Validate Configuration(**구성 검토 및 검증**)** 화면에서 **Access Control Rules(**액세스 제어 규칙**)**를 클릭하고 다음과 같이 합니다.

a) 테이블의 각 항목에 대해 매핑을 검토하고 올바른지 확인합니다.

마이그레이션된 액세스 정책 규칙은 ACL 이름을 접두사로 사용하고 ACL 규칙 번호를 추가하므로 FDM 매니지드 디바이스 구성 파일에 다시 쉽게 매핑할 수 있습니다. 예를 들어 FDM 매니지드 디바이스 ACL의 이름이 "inside_access"인 경우 ACL의 첫 번째 규칙(또는 ACE) 라인은 "inside_access_# 1"로 지정됩니다. TCP 또는 UDP 조합, 확장된 서비스 개체 또는 기타 사유로 인해 규칙을 확장해야 하는 경우 Secure Firewall 마이그레이션 툴이 이름에 번호가 지정된 접미사를 추가합니다. 예를 들어 허용 규칙이 마이그레이션을 위해 두 개의 규칙으로 확장되는 경우 이름이 "inside_access _#1-1"및 "inside_access_#1-2"로 지정됩니다.

지원되지 않는 개체를 포함하는 규칙의 경우 Secure Firewall 마이그레이션 툴이 이름에 "_UNSUPPORTED" 접미사를 추가합니다.

b) 하나 이상의 액세스 제어 목록 정책을 마이그레이션하지 않으려면 해당 행의 체크 박스를 선택하고 **Actions(**작업**)** > **Do not migrate(**마이그레이션하지 않음**)**을 선택한 다음 **Save(**저장**)**를 클릭합니다.

마이그레이션하지 않도록 선택하는 모든 규칙은 테이블에서 회색으로 표시됩니다.

c) 하나 이상의 액세스 제어 정책에 management center 파일 정책을 적용하려면 해당 행의 체크 박스를 선택하고 **Actions(**작업**)** > **File Policy(**파일 정책**)**를 선택합니다.

File Policy(파일 정책**)** 대화 상자에서 적절한 파일 정책을 선택하고 선택한 액세스 제어 정책에 적용한 후 **Save(**저장**)**를 클릭합니다.

d) 하나 이상의 액세스 제어 정책에 management center IPS 정책을 적용하려면 해당 행의 체크 박스를 선택하고 **Actions(**작업**)** > **IPS Policy(IPS** 정책**)**를 선택합니다.

IPS Policy(IPS 정책**)** 대화 상자에서 적절한 IPS 정책과 해당 변수 집합을 선택하고 선택한 액세스 제어 정책에 적용한 후 **Save(**저장**)**를 클릭합니다.

e) 기록이 활성화된 액세스 제어 규칙의 기록 옵션을 변경하려면 해당 행의 체크 박스를 선택하고 **Actions(**작업**)** > **Log(**로그**)**를 선택합니다.

Log(로그**)** 대화 상자에서 연결 시작 또는 종료 시 또는 두 경우에 모두 이벤트 기록을 활성화할 수 있습니다. 기록을 활성화한 경우 **Event Viewer(**이벤트 뷰어**)** 또는 **Syslog(**시스템 로그**)** 또는 둘 다에 연결 이벤트를 보내도록 선택해야 합니다. 시스템 로그 서버에 연결 이벤트를 전송하도록 선택하는 경우 **Syslog(**시스템 로그**)** 드롭다운 메뉴에서 management center에 이미 구성된 시스템 로그 정책을 선택할 수 있습니다.

f) 액세스 제어 테이블에서 마이그레이션된 액세스 제어 규칙에 대한 작업을 변경하려면 해당 행의 체크 박스를 선택하고 **Actions(**작업**)** > **Rule Action(**규칙 작업**)**을 선택합니다.

Actions(작업**)** 드롭다운의 **Rule Action(**규칙 작업**)** 대화 상자에서 **ACP** 또는 **Prefilter(**사전 필터**)** 탭을 선택할 수 있습니다.

- ACP - 모든 액세스 제어 규칙에는 시스템이 일치하는 트래픽을 처리하고 기록하는 방법을 결정하는 작업이 있습니다. 액세스 제어 규칙에 대해 허용, 신뢰, 모니터링, 차단 또는 차단 후 재설정 작업을 수행할 수 있습니다.
- Prefilter(사전 필터) - 규칙의 작업은 시스템이 일치하는 트래픽을 처리하고 기록하는 방법을 결정합니다. 단축경로(Fastpath) 지정 및 차단을 수행할 수 있습니다.

팁 액세스 제어 규칙에 연결된 IPS 및 파일 정책은 Allow(허용) 옵션을 제외한 모든 규칙 작업 시 자동으로 제거됩니다.

정책 용량 및 제한 경고 - Secure Firewall 마이그레이션 툴은 마이그레이션된 규칙의 총 ACE 수를 대상 플랫폼에서 지원되는 ACE 제한과 비교합니다.

비교 결과를 기반으로 Secure Firewall 마이그레이션 툴은 마이그레이션된 ACE의 총 수가 임계값을 초과하거나 대상 디바이스의 지원되는 제한 임계값에 근접한 경우 가시적인 지표 및 경고 메시지를 표시합니다.

규칙이 ACE Count(ACE 수) 열을 초과할 경우 마이그레이션을 최적화하거나 마이그레이션하지 않도록 결정할 수 있습니다. 구축 전에 management center에서 푸시한 후 마이그레이션을 완료하고 이 정보를 사용하여 규칙을 최적화할 수도 있습니다.

참고 Secure Firewall 마이그레이션 툴은 경고에도 불구하고 마이그레이션을 차단하지 않습니다.

이제 오름차순, 내림차순, 같음, 보다 큼, 보다 작음 필터링 순서 시퀀스로 ACE 수를 필터링할 수 있습니다.

기존 필터 기준을 지우고 새 검색을 로드하려면 **Clear Filter(**필터 지우기**)**를 클릭합니다.

참고 ACE를 기준으로 ACL을 정렬하는 순서는 보기 전용입니다. ACL은 발생한 연대순으로 푸시됩니다.

g) 침입 정책에는 모든 침입 정책 및 해당 기본 정책, 존재하는 사용자 지정/재정의 규칙, ACP의 침입 모드 및 참조가 표시됩니다. Snort 3에 대한 Snort 엔진 및 NAP 정책도 표시됩니다.

재정의된 규칙이 있는 Snort 2 정책은 Management Center의 API 제한으로 인해 무시됩니다.

기본 설정의 침입 정책은 Management Center에서 재사용됩니다.

Snort 3 또는 Snort3/Snort2에 대한 침입 모드 탐지에 대해 재정의된 규칙/사용자 지정 규칙이 있는 침입 정책용 정책 이름이 _ <FDM Hostname>인 새 정책이 생성됩니다.

단계 **3** 다음 탭을 클릭하고 컨피그레이션 항목을 검토합니다.

- **NAT** 규칙
- 개체**(**액세스 목록 개체**,** 네트워크 개체**,** 포트 개체**, VPN** 개체 및 유동 경로 개체**)**
- 인터페이스
- 경로
- 사이트 대 사이트 **VPN** 터널
- 원격 액세스 **VPN**

액세스 목록 개체는 BGP, EIGRP, RA VPN에서 사용되는 표준 및 확장 ACL을 표시합니다.

하나 이상의 NAT 규칙 또는 라우팅 인터페이스를 마이그레이션하지 않으려면 해당 행의 체크 박스를 선택하고 **Actions(**작업**)** > **Do not migrate(**마이그레이션하지 않음**)**을 선택한 다음 **Save(**저장**)**를 클릭합니다.

마이그레이션하지 않도록 선택하는 모든 규칙은 테이블에서 회색으로 표시됩니다.

단계 **4** (선택 사항) 컨피그레이션을 검토하는 동안 **Network Objects(**네트워크 개체**)** 탭 또는 **Port Objects(**포트 개체**)** 탭 또는 **VPN Objects(VPN** 개체**)**에서 **Actions(**작업**)** > **Rename(**이름 바꾸기**)**을 선택하여 하나 이상의 네트워크, 포트 또는 VPN 개체의 이름을 변경할 수 있습니다.

이름이 변경된 개체를 참조하는 액세스 규칙 및 NAT 정책도 새 개체 이름으로 업데이트됩니다.

단계 **5** **Remote Access VPN(**원격 액세스 **VPN)** 섹션에서는 원격 액세스 VPN에 해당하는 모든 개체가 FDM 매니지드 디바이스에서 Management Center로 마이그레이션되며 다음과 같이 표시됩니다.

- **AnyConnect** 파일 - AnyConnect 패키지, Hostscan 파일(Dap.xml, Data.xml, Hostscan 패키지), 외부 브라우저 패키지 및 AnyConnect 프로파일은 소스 FDM 매니지드 디바이스에서 검색해야 하며 마이그레이션에 사용할 수 있어야 합니다.

  마이그레이션 전 작업의 일부로 모든 AnyConnect 패키지를 Management Center에 업로드합니다. AnyConnect 프로파일을 Management Center에 직접 업로드하거나 Secure Firewall 마이그레이션 툴에서 업로드할 수 있습니다.

Management Center에서 가져온 기존 AnyConnect, Hostscan 또는 외부 브라우저 패키지를 선택합니다. AnyConnect 패키지를 하나 이상 선택해야 합니다. Hostscan, dap.xml, data.xml 또는 외부 브라우저(소스 구성에서 사용 가능한 경우)를 선택해야 합니다. AnyConnect 프로파일은 선택 사항입니다.

Dap.xml은 FDM 매니지드 디바이스에서 검색된 올바른 파일이어야 합니다. 구성 파일에 있는 dap.xml에 대해 검증이 수행됩니다. 검증에 필요한 모든 파일을 업로드하고 선택해야 합니다. 업데이트에 실패하면 완료되지 않은 것으로 표시되고 Secure Firewall 마이그레이션 툴이 검증을 진행하지 않습니다.

- **AAA** - Radius, LDAP, AD, LDAP, SAML 및 Local Realm(로컬 영역) 유형의 인증 서버가 표시됩니다. 모든 AAA 서버의 키를 업데이트합니다. Secure Firewall 마이그레이션 툴 3.0부터는 Live Connect FDM 매니지드 디바이스에 대해 사전 공유 키가 자동으로 검색됩니다. **more system: running-config** 파일을 사용하여 숨겨진 키와 함께 소스 구성을 업로드할 수도 있습니다. 일반 텍스트 형식의 AAA 인증 키를 검색하려면 다음 단계를 수행합니다.

  참고 이러한 단계는 Secure Firewall 마이그레이션 툴 외부에서 수행해야 합니다.

  1. SSH 콘솔을 통해 FDM 매니지드 디바이스에 연결합니다.
  2. *more system:running-config* 명령을 입력합니다.
  3. **aaa-server and local user(aaa-server** 및 로컬 사용자**)** 섹션으로 이동하여 일반 텍스트 형식의 모든 AAA 구성 및 각 키 값을 찾습니다.

```
ciscoFDM#more system:running-config
!
aaa-server Test-RADIUS (inside) host 2.2.2.2
key <key in clear text> <-----The radius key is now displayed in clear text format. aaa-server
Test-LDAP (inside) host 3.3.3.3
ldap-login-password <Password in clear text> <-----TheLDAP/AD/LDAPS password is now displayed in
 clear text format.
username Test_User password <Password in clear text> <-----The Local user password is shown in
clear text.
```

  참고 로컬 사용자의 비밀번호가 암호화된 경우 내부에서 비밀번호를 확인하거나 Secure Firewall 마이그레이션 툴에서 새 비밀번호를 구성할 수 있습니다.

- LDAPS에는 Management Center의 도메인이 필요합니다. 암호화 유형 LDAPS에 대한 도메인을 업데이트해야 합니다.
- AD 서버에는 management center에 고유한 AD 기본 도메인이 필요합니다. 고유한 도메인이 식별되면 Secure Firewall 마이그레이션 툴에 표시됩니다. 충돌이 발견되면 사용자는 고유한 AD 기본 도메인을 입력해야 개체를 푸시할 수 있습니다.

  암호화가 LDAPS로 설정된 AAA 서버의 경우 FDM 매니지드 디바이스는 IP 및 호스트 이름 또는 도메인을 지원하지만, Management Center는 호스트 이름 또는 도메인만 지원합니다. FDM 매니지드 디바이스 구성에 호스트 이름 또는 도메인이 포함된 경우 검색되어 표시됩니다. FDM 매니지드 디바이스 구성에 LDAPS용 IP 주소가 포함된 경우 **Remote Access VPN(**원격 액세스 **VPN)** 아래의 **AAA** 섹션에 도메인을 입력합니다. AAA 서버의 IP 주소로 확인할 수 있는 도메인을 입력해야 합니다.

  유형이 AD인 AAA 서버의 경우(서버 유형은 FDM 매니지드 디바이스 구성에서 Microsoft임) **AD Primary Domain(AD** 기본 도메인**)**은 Management Center에서 구성해야 하는 필수 필드입니다. 이 필드는 FDM 매니지드 디바이스에서 별도로 구성되지 않으며 FDM 매니지드 디바이스의 LDAP-base-dn 구성에서 추출됩니다.

`ldap-base-dn이 ou=Test-Ou,dc=gcevpn,dc=com인 경우`

AD Primary Domain(AD 기본 도메인**)**은 기본 도메인을 구성하는 dc, dc=gcevpn 및 dc=com으로 시작하는 필드입니다. AD 기본 도메인은 gcevpn.com입니다.

LDAP-base-dn 예시 파일:

```
cn=FDM,OU=ServiceAccounts,OU=abc,dc=abc,dc=com:
```

여기서 dc=abc 및 dc=com은 abc.com으로 결합되어 AD 기본 도메인을 형성합니다.

```
cn=admin, cn=users, dc=fwsecurity, dc=cisco, dc=com:
```

AD 기본 도메인은 fwsecurity.cisco.com입니다.

AD 기본 도메인이 자동으로 검색되어 Secure Firewall 마이그레이션 툴에 표시됩니다.

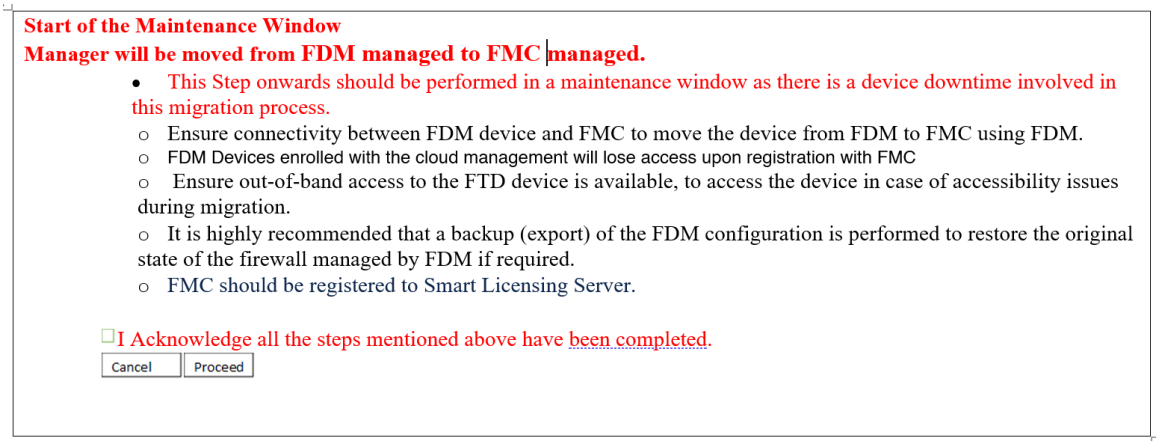
참고 AD 기본 도메인 값은 각 영역 개체에 대해 고유해야 합니다. 충돌이 탐지되거나 Firewall 마이그레이션 툴이 FDM 매니지드 디바이스 구성에서 값을 찾을 수 없는 경우, 특정 서버에 대한 AD 기본 도메인을 입력하라는 메시지가 표시됩니다. 구성을 검증할 AD 기본 도메인을 입력합니다.

- **Address Pool(**주소 풀**)**-모든 Ipv4 및 Ipv6 풀이 여기에 표시됩니다.
- **Group-Policy(**그룹 정책**)**-이 섹션에는 클라이언트 프로파일이 있는 그룹 정책, 관리 프로파일, 클라이언트 모듈 및 프로파일이 없는 그룹 정책이 표시됩니다. 프로파일이 AnyConnect file(AnyConnect 파일) 섹션에 추가된 경우 사전 선택된 것으로 표시됩니다. 사용자 프로파일, 관리 프로파일 및 클라이언트 모듈 프로파일을 선택하거나 제거할 수 있습니다.
- **Connection Profile(**연결 프로파일**)**-모든 연결 프로파일/터널 그룹이 여기에 표시됩니다.
- **Trustpoint(**트러스트 포인트**)**-FDM 매니지드 디바이스에서 Management Center로의 트러스트 포인트 또는 PKI 개체 마이그레이션은 마이그레이션 전 활동의 일부이며 RA VPN을 성공적으로 마이그레이션하는 데 필요합니다. **Remote Access Interface(**원격 액세스 인터페이스**)** 섹션에서 전역 SSL, IKEv2 및 인터페이스에 대한 트러스트 포인트를 매핑하여 다음 마이그레이션 단계를 진행합니다. LDAPS 프로토콜이 활성화된 경우 전역 SSL 및 IKEv2 트러스트 포인트는 필수입니다. SAML 개체가 존재하는 경우 SAML 섹션에서 SAML IDP 및 SP에 대한 트러스트 포인트를 매핑할 수 있습니다. SP 인증서는 선택 사항입니다. 특정 터널 그룹에 대해 트러스트 포인트를 재정의할 수도 있습니다. 재정의된 SAML 트러스트 포인트 구성을 소스 FDM 매니지드 디바이스에서 사용할 수 있는 경우 **Override SAML(SAML** 재정의**)** 옵션에서 선택할 수 있습니다.

  FDM 매니지드 디바이스에서 PKI 인증서를 내보내는 방법에 대한 자세한 내용은 FDM 매니지드 디바이스 구성 파일 내보내기를 참고하십시오.
- **Certificate Maps(**인증서 맵**)**- 여기에는 인증서 맵이 표시됩니다.

유지 보수 및 이동 관리자 시작

공유 구성이 푸시되면 팝업을 수락하여 유지 보수 창으로 이동해야 합니다.



Move Manager(이동 관리자**)** 페이지에 다음 세부 정보를 입력해야 합니다.

- **FTD is behind NAT Device(FTD**가 **NAT** 디바이스 이면에 있음**), FMC is behind NAT Device(FMC**가 **NAT** 디바이스 이면에 있음**), No Device is behind NAT(Default Setting)(**디바이스가 **NAT** 이면에 없음**(**기본 설정**))** 중에서 선택합니다.
- **Management Center/CDO Hostname or IP Address(Management Center/CDO** 호스트 이름 또는 **IP** 주소**)**: 모든 세부 정보를 대상 관리자에서 가져옵니다. 필요한 경우 IP를 수정할 수 있습니다.

참고 **FMC is behind NAT Device(FMC**가 **NAT** 디바이스 이면에 있음**)**를 선택한 경우 필드가 무시됩니다.

- **Management Center/CDO Registration Key(Management Center/CDO** 등록 키**)**: 관리자를 이동하는 동안 사용할 고유한 등록 키를 제공해야 합니다.
- **NAT ID**: (선택 사항) Threat Defense 또는 Management Center가 NAT 디바이스 이면에 있는 경우 필수입니다.
- **Threat Defense (FTD) Hostname(Threat Defense(FTD)** 호스트 이름**)**: FDM 매니지드 디바이스 구성에서 Threat Defense IP/호스트 이름을 가져옵니다. 사용자는 필요한 경우 IP를 수정할 수 있습니다. **FTD is behind NAT Device(FTD**가 **NAT** 디바이스 이면에 있음**)**를 선택한 경우 필드가 무시됩니다.
- **DNS Server Group(DNS** 서버 그룹**)**: Device Manager와 Management Center 간의 연결에 사용되는 DNS 서버 그룹입니다.
- **Management Center/ CDO Access Interface (Data/Management)(Management Center/CDO** 액세스 인터페이스**(**데이터/관리**))**: 관리자를 이동할 데이터/관리 인터페이스 중에서 선택합니다. 데이터 인터페이스는 데이터 인터페이스를 통해 적절한 경로가 구성된 경우에만 지원됩니다.

Move Manager(관리자 이동**)**를 선택하면 Secure Firewall 마이그레이션 툴이 Device Manager에서 Management Center로 관리자를 이동합니다. 관리자를 이동한 후에는 Device Manager에서 디바이스에 액세스할 수 없습니다.

마이그레이션할 디바이스 컨피그레이션 최적화, 검토 및 검증

단계 **1** 다음 탭을 선택하고 구성 항목을 검토합니다.

- 인터페이스
- 경로
- 사이트 대 사이트 **VPN** 터널

Dynamic-Route-Objects(유동 경로 개체**)** 섹션에 마이그레이션되는 모든 지원 개체가 표시됩니다.

- Policy-List
- Prefix-List
- Route-Map
- 커뮤니티 목록
- AS-Path
- Access-List

단계 **2** **Routes(**경로**)** 섹션에 다음 경로가 표시됩니다.

- Static(정적) - 모든 IPv4 및 IPv6 정적 경로를 표시합니다.
- BGP — 모든 BGP 경로를 표시합니다.
- EIGRP - 모든 EIGRP 경로를 표시합니다. EIGRP의 경우 more system:running 구성이 업로드되고 키가 암호화되지 않은 경우 인증 키를 가져옵니다. 키가 소스 구성에서 암호화된 경우 EIGRP의 Interface(인터페이스) 섹션에서 키를 수동으로 제공할 수 있습니다. 인증 유형(encrypted(암호화됨), unencrypted(암호화되지 않음), auth(인증됨) 또는 none(없음))을 선택하고 그에 따라 키를 제공합니다.

단계 **3** 검토를 완료한 후 **Validate(**검증**)**를 클릭합니다.

검증 과정에서 Secure Firewall 마이그레이션 툴은 Management Center에 연결하여 기존 개체를 검토하고 마이그레이션할 개체 목록과 비교합니다. 개체가 이미 Management Center에 있는 경우 Secure Firewall 마이그레이션 툴은 다음과 같이 합니다.

- 개체의 이름과 구성이 동일한 경우 Secure Firewall 마이그레이션 툴은 기존 개체를 재사용하고 Management Center에 새 개체를 생성하지 않습니다.
- 개체의 이름은 같지만 구성이 다른 경우 Secure Firewall 마이그레이션 툴이 개체 충돌을 보고합니다.

콘솔에서 검증 진행 상황을 볼 수 있습니다.

단계 **4** 검증이 완료된 후 **Validation Status(**검증 상태**)** 대화 상자에 하나 이상의 개체 충돌이 표시되면 다음과 같이 합니다.

a) **Resolve Conflicts(**충돌 해결**)**를 클릭합니다.

Secure Firewall 마이그레이션 툴은 개체 충돌이 보고된 위치에 따라 **Network Objects(**네트워크 개체**)** 또는 **Port Objects(**포트 개체**)** 탭 중 하나 또는 둘 다에 경고 아이콘을 표시합니다.

b) 탭을 클릭하고 개체를 검토합니다.
c) 충돌이 있는 각 개체의 항목을 확인하고 **Actions(**작업**)** > **Resolve Conflicts(**충돌 해결**)**를 선택합니다.
d) **Resolve Conflicts(**충돌 해결**)** 창에서 권장 작업을 완료합니다.

예를 들어, 기존 management center 개체와의 충돌을 방지하기 위해 개체 이름에 접미사를 추가하라는 메시지가 표시될 수 있습니다. 기본 접미사를 수락하거나 자체 접미사로 대체할 수 있습니다.

e) **Resolve(**해결**)**를 클릭합니다.
f) 탭에서 모든 개체 충돌을 해결했으면 **Save(**저장**)**를 클릭합니다.
g) **Validate(**검증**)**를 클릭하여 컨피그레이션을 재검증하고 모든 개체 충돌이 해결되었는지 확인합니다.

단계 **5** 검증이 완료되고 **Validation Status(**검증 상태**)** 대화 상자에 **Successfully Validated(**검증 성공**)** 메시지가 표시되면 Push the Migrated Configuration to Management Center(Management Center로 마이그레이션된 구성 푸시)로 진행합니다.

마이그레이션된 컨피그레이션을 Management Center에 푸시

구성을 성공적으로 검증하고 모든 개체 충돌을 해결하지 않은 경우 마이그레이션된 FDM 매니지드 디바이스 구성을 management center에 푸시할 수 없습니다.

마이그레이션 프로세스의 이 단계에서는 마이그레이션된 컨피그레이션을 management center에 보냅니다. Threat Defense 디바이스에 컨피그레이션이 구축되지는 않습니다. 하지만 Threat Defense의 모든 기존 컨피그레이션이 이 단계에서 지워집니다.

참고 Secure Firewall 마이그레이션 툴이 마이그레이션된 구성을 management center에 보내는 동안에는 구성을 변경하거나 디바이스에 구축하지 마십시오.

단계 **1** **Validation Status(**검증 상태**)** 대화 상자에서 검증 요약을 검토합니다.

단계 **2** **Push Configuration(**구성 푸시**)**을 클릭하여 마이그레이션된 FDM 매니지드 디바이스 구성을 management center에 보냅니다.

Secure Firewall 마이그레이션 툴의 새로운 최적화 기능을 통해 검색 필터를 사용하여 마이그레이션 결과를 빠르게 가져올 수 있습니다.

또한 Secure Firewall 마이그레이션 툴은 CSV 다운로드를 최적화하고 페이지 보기별로 또는 모든 규칙에 작업을 적용할 수 있도록 지원합니다.

Secure Firewall 마이그레이션 툴에 마이그레이션 진행 상황의 요약이 표시됩니다. 콘솔에서 management center에 푸시되는 구성 요소의 세부적인 라인별 진행 상황을 볼 수 있습니다.

단계 **3** 마이그레이션이 완료되면 **Download Report(**보고서 다운로드**)**를 클릭하여 마이그레이션 후 보고서를 다운로드하고 저장합니다.

Post-Migration Report(마이그레이션 후 보고서**)**의 사본도 Secure Firewall 마이그레이션 툴과 동일한 위치의 `Resources` 폴더에 저장됩니다.

단계 **4** 마이그레이션이 실패한 경우 마이그레이션 후 보고서, 로그 파일, 구문 분석되지 않은 파일을 신중하게 검토하여 실패의 원인을 파악합니다.

문제 해결을 위해 지원 팀에 문의할 수도 있습니다.

마이그레이션 실패 지원

마이그레이션이 실패할 경우 지원 팀에 문의합니다.

1. **Complete Migration(**마이그레이션 완료**)** 화면에서 **Support(**지원**)** 버튼을 클릭합니다.

   도움말 지원 페이지가 나타납니다.

2. **Support Bundle(**지원 번들**)** 체크 박스를 선택한 다음 다운로드할 컨피그레이션 파일을 선택합니다.

   참고 로그 및 dB 파일은 기본적으로 다운로드하도록 선택됩니다.

3. **Download(**다운로드**)**를 클릭합니다.

   지원 번들 파일은 로컬 경로에 .zip으로 다운로드됩니다. 압축 폴더의 압축을 풀고 로그 파일, DB 및 컨피그레이션 파일을 봅니다.

4. **Email us(**이메일 문의**)**를 클릭하여 기술 팀에 실패 세부 정보를 이메일로 보냅니다.

   다운로드한 지원 파일을 이메일에 첨부할 수도 있습니다.

5. **Visit TAC page(TAC** 페이지 방문**)**를 클릭하여 Cisco 지원 페이지에서 TAC 케이스를 생성합니다.

   참고 마이그레이션하는 동안 언제라도 지원 페이지에서 TAC 케이스를 열 수 있습니다.

마이그레이션 후 보고서 검토 및 마이그레이션 완료

마이그레이션 후 보고서는 다양한 범주의 ACL 수, ACL 최적화 및 컨피그레이션 파일에서 수행된 최적화의 전체 보기에 대한 세부 정보를 제공합니다. 자세한 내용은 마이그레이션할 컨피그레이션 최적화, 검토 및 검증, 23 페이지을 참조해 주십시오.

개체를 검토하고 확인합니다.

- 카테고리
  - 총 ACL 규칙(소스 컨피그레이션)
  - 최적화를 위해 고려된 총 ACL 규칙. 예를 들어, 중복, 섀도우 등이 있습니다.
- 최적화할 ACL 수는 최적화 전후에 계산한 총 ACL 규칙 수를 제공합니다.

마이그레이션 중에 마이그레이션 후 보고서를 다운로드하지 못한 경우 다음 링크를 사용하여 다운로드하십시오.

마이그레이션 후 보고서 다운로드 엔드포인트 - http://localhost:8888/api/downloads/post_migration_summary_html_format

참고 Secure Firewall 마이그레이션 툴이 실행 중일 때만 보고서를 다운로드할 수 있습니다.

단계 1 **Post-Migration Report(**마이그레이션 후 보고서**)**를 다운로드한 위치로 이동합니다.

단계 2 마이그레이션 후 보고서를 열고 내용을 신중하게 검토하여 FDM 매니지드 디바이스 구성이 어떻게 마이그레이션되었는지 파악합니다.

- **Migration Summary(**마이그레이션 요약**)** - FDM 매니지드 디바이스에서 Threat Defense로 성공적으로 마이그레이션된 구성의 요약으로, FDM 매니지드 디바이스 인터페이스, management center 호스트 이름 및 도메인, 대상 Threat Defense 디바이스 (적용 가능한 경우) 및 성공적으로 마이그레이션된 구성 요소에 대한 정보가 포함됩니다.
- **FDM Migration Path(FDM** 마이그레이션 경로**)** - 3가지 마이그레이션 플로우 중에서 선택된 옵션을 표시합니다.
  - **Firepower Device Manager** 마이그레이션**(**공유 구성만 해당**)**
  - **Firepower Device Manager** 마이그레이션**(**디바이스 및 공유 구성 포함**)**
  - **Firepower Device Manager(**디바이스 및 공유 구성 포함**)**를 **FTD** 디바이스**(**새 하드웨어**)**로 마이그레이션
- **Selective Policy Migration(**선택적 정책 마이그레이션**)** - 마이그레이션하도록 선택한 특정 FDM 매니지드 디바이스 기능에 대한 세부 정보를 Device Configuration Features(디바이스 구성 기능), Shared Configuration Features(공유 구성 기능), Optimization(최적화)의 세 범주에서 확인할 수 있습니다.
- **FDM-managed device Interface to Threat Defense Interface Mapping**(ASA FPS 포함 ASA FDM 매니지드 디바이스 인터페이스-Threat Defense 인터페이스 매핑) - 성공적으로 마이그레이션된 인터페이스와 FDM 매니지드 디바이스 구성의 인터페이스를 Threat Defense 디바이스의 인터페이스에 매핑한 방법에 대한 세부 정보입니다. 이러한 매핑이 예상과 일치하는지 확인합니다.

  참고 이 섹션은 마이그레이션에 대상 Threat Defense 디바이스가 없는 경우 또는 인터페이스를 마이그레이션하도록 선택하지 않은 경우에는 적용되지 않습니다.

- **Source Interface Names to Threat Defense Security Zones and Interface Groups(**소스 인터페이스 이름**-Threat Defense** 보안 영역 및 인터페이스 그룹**)** - 성공적으로 마이그레이션된 FDM 매니지드 디바이스 논리적 인터페이스 및 이름과 Threat Defense에서 이를 보안 영역 및 인터페이스 그룹에 매핑한 방법에 대한 세부 정보입니다. 이러한 매핑이 예상과 일치하는지 확인합니다.

  참고 **Access Control Lists(**액세스 제어 목록**)** 및 **NAT**가 마이그레이션하도록 선택되지 않은 경우 이 섹션은 적용되지 않습니다.

- **Object Conflict Handling(**개체 충돌 처리**)** - management center의 기존 개체와 충돌하는 것으로 확인된 FDM 매니지드 디바이스 개체에 대한 세부 정보입니다. 개체의 이름과 구성이 동일한 경우 Secure Firewall 마이그레이션 툴에서 management center 개체를 재사용했습니다. 개체의 이름은 같지만 컨피그레이션이 다른 경우 해당 개체의 이름을 변경했습니다. 이러한 개체를 신중하게 검토하고 충돌이 적절하게 해결되었는지 확인합니다.

- **Access Control Rules, NAT, and Routes You Chose Not to Migrate(**마이그레이션하지 않도록 선택한 액세스 제어 규칙**, NAT** 및 경로**)** - Secure Firewall 마이그레이션 툴을 사용하여 마이그레이션하지 않도록 선택한 규칙에 대한 세부 정보입니다. Secure Firewall 마이그레이션 툴에서 비활성화되고 마이그레이션되지 않은 이러한 규칙을 검토합니다. 이러한 라인을 검토하고 선택한 모든 규칙이 이 섹션에 나열되어 있는지 확인합니다. 원하는 경우 이러한 규칙을 수동으로 구성할 수 있습니다.
- **Partially Migrated Configuration(**부분적으로 마이그레이션된 구성**)** - 고급 옵션이 포함되어 있지만 고급 옵션 없이 마이그레이션될 수 있는 규칙을 비롯하여 부분적으로만 마이그레이션된 FDM 매니지드 디바이스 규칙에 대한 세부 정보입니다. 이러한 라인을 검토하고 management center에서 고급 옵션이 지원되는지 확인한 다음 지원되는 경우 해당 옵션을 수동으로 구성합니다.
- **Unsupported Configuration(**지원되지 않는 구성**)** - Secure Firewall 마이그레이션 툴이 해당 기능의 마이그레이션을 지원하지 않으므로 마이그레이션할 수 없는 FDM 매니지드 디바이스 구성 요소에 대한 세부 정보입니다. 이러한 라인을 검토하여 각 기능이 Threat Defense에서 지원되는지 확인합니다. 지원되는 경우 management center에서 해당 기능을 수동으로 구성합니다.
- **Expanded Access Control Policy Rules(**확장 액세스 제어 정책 규칙**)**- 마이그레이션 중에 단일 FDM 매니지드 디바이스 포인트 규칙에서 여러 Threat Defense 규칙으로 확장된 FDM 매니지드 디바이스 액세스 제어 정책 규칙에 대한 세부 정보입니다.
- **Actions Taken on Access Control Rules(**액세스 제어 규칙에 대해 수행된 작업**)**
  - **Access Rules You Chose Not to Migrate(**마이그레이션하지 않도록 선택한 액세스 규칙**)** - Secure Firewall 마이그레이션 툴을 사용하여 마이그레이션하지 않도록 선택한 FDM 매니지드 디바이스 액세스 제어 규칙에 대한 세부 정보입니다. 이러한 라인을 검토하고 선택한 모든 규칙이 이 섹션에 나열되어 있는지 확인합니다. 원하는 경우 이러한 규칙을 수동으로 구성할 수 있습니다.
  - **Access Rules with Rule Action Change(**규칙 작업이 변경된 액세스 규칙**)** - Secure Firewall 마이그레이션 툴을 사용하여 '규칙 작업'이 변경된 모든 액세스 제어 정책 규칙에 대한 세부 정보입니다. 규칙 작업 값은 Allow(허용), Trust(신뢰), Monitor(모니터링), Block(차단), Block with reset(차단 후 재설정)입니다. 이러한 라인을 검토하고 선택한 모든 규칙이 이 섹션에 나열되어 있는지 확인합니다. 원하는 경우 이러한 규칙을 수동으로 구성할 수 있습니다.
  - **Access Control Rules that have IPS Policy and Variable Set Applied(IPS** 정책 및 변수 집합이 적용된 액세스 제어 규칙**)** - IPS 정책이 적용된 모든 FDM 매니지드 디바이스 액세스 제어 정책 규칙에 대한 세부 정보입니다. 이러한 규칙을 신중하게 검토하고 Threat Defense에서 해당 기능이 지원되는지 확인합니다.
  - **Access Control Rules that have File Policy Applied(**파일 정책이 적용된 액세스 제어 규칙**)** - 파일 정책이 적용된 모든 FDM 매니지드 디바이스 액세스 제어 정책 규칙에 대한 세부 정보입니다. 이러한 규칙을 신중하게 검토하고 Threat Defense에서 해당 기능이 지원되는지 확인합니다.
  - **Access Control Rules that have Rule 'Log' Setting Change(**규칙 '로그' 설정이 변경된 액세스 제어 규칙**)** - Secure Firewall 마이그레이션 툴을 사용하여 '로그 설정'이 변경된 FDM 매니지드 디바이스 액세스 제어 규칙에 대한 세부 정보입니다. 로그 설정 값은 False(거짓), Event Viewer(이벤트 뷰어), Syslog(시스템 로그)입니다. 이러한 라인을 검토하고 선택한 모든 규칙이 이 섹션에 나열되어 있는지 확인합니다. 원하는 경우 이러한 규칙을 수동으로 구성할 수 있습니다.

참고 마이그레이션되지 않은 지원되지 않는 규칙은 원치 않는 트래픽이 방화벽을 통과하는 문제를 일으킵니다. 이 트래픽이 Threat Defense에서 차단되도록 management center에서 규칙을 구성하는 것이 좋습니다.

참고 **Review and Validate(**검토 및 검증**)** 페이지에서 ACL에 IPS 또는 파일 정책을 적용해야 하는 경우 마이그레이션 전에 관리 센터에서 정책을 생성하는 것이 좋습니다. Secure Firewall 마이그레이션 툴이 연결된 Management Center에서 정책을 가져오므로 동일한 정책을 사용합니다. 새 정책을 생성하고 여러 정책에 할당하면 성능이 저하될 수 있으며 푸시가 실패할 수도 있습니다.

management center 및 Threat Defense에서 지원되는 기능에 대한 자세한 내용은 Management Center 컨피그레이션 가이드, 버전 6.2.3을 참고하십시오.

단계 **3** **Pre-Migration Report(**마이그레이션 전 보고서**)**를 열고 Threat Defense 디바이스에서 수동으로 마이그레이션해야 하는 FDM 매니지드 디바이스 구성 항목을 기록해 둡니다.

단계 **4** management center에서 다음과 같이 합니다.

a) Threat Defense 디바이스에 대해 마이그레이션된 컨피그레이션을 검토하여 다음을 비롯한 모든 예상 규칙 및 기타 컨피그레이션 항목이 마이그레이션되었는지 확인합니다.

- ACL(액세스 제어 목록)
- NAT(Network Address Translation) 규칙
- 포트 및 네트워크 개체
- 경로
- 인터페이스
- IP SLA 개체
- 개체 그룹 검색
- 시간 기반 개체
- 사이트 대 사이트 VPN 터널
- 유동 경로 개체

b) 마이그레이션되지 않은 부분적으로 지원되는 항목 및 규칙, 지원되지 않는 항목 및 규칙, 무시된 항목 및 규칙, 비활성화된 항목 및 규칙을 모두 구성합니다.

이러한 항목 및 규칙에 대한 정보는 Management Center 컨피그레이션 가이드를 참고하십시오. 다음은 수동 구성이 필요한 컨피그레이션 항목의 예입니다.

- Threat Defense의 플랫폼 설정에 설명된 SSH 및 HTTPS 액세스를 포함한 플랫폼 설정
- 시스템 로그 구성에 설명된 시스템 로그 설정
- Threat Defense 라우팅 개요에 설명된 동적 라우팅
- FlexConfig 정책에 설명된 서비스 정책
- Threat Defense VPN에 설명된 VPN 컨피그레이션
- 연결 기록에 설명된 연결 로그 설정

마이그레이션 전에 AD 영역의 암호화를 변경한 경우 아래 단계에 따라 암호화 유형을 LDAPS 또는 STARTTLS로 되돌립니다.

1. **Integration(**통합**)** 섹션으로 이동하여 **Other Integrations(**기타 통합**)**를 클릭합니다.
2. 암호화 유형을 변경하려면 **Realms(**영역**)**를 선택하고 특정 영역 옆에 있는 **Edit(**수정**)** (✎) 아이콘을 클릭합니다.
3. **Directory(**디렉터리**)**를 클릭하고 암호화 유형을 **LDAPS** 또는 **STARTTLS**로 변경합니다.
4. 변경 사항을 저장 및 구축합니다.

단계 **5** 검토를 완료한 후 마이그레이션된 컨피그레이션을 management center에서 Threat Defense 디바이스로 구축합니다.

지원되지 않는 규칙과 부분적으로 지원되는 규칙에 대한 데이터가 **Post-Migration Report(**마이그레이션 후 보고서**)**에 올바르게 반영되어 있는지 확인합니다.

Secure Firewall 마이그레이션 툴이 Threat Defense 디바이스에 정책을 할당합니다. 변경 사항이 실행 중인 컨피그레이션에 반영되어 있는지 확인합니다. 마이그레이션되는 정책을 쉽게 식별할 수 있도록 해당 정책의 설명에 FDM 매니지드 디바이스 구성의 호스트 이름이 포함되어 있습니다.

Secure Firewall 마이그레이션 툴 제거

모든 구성 요소는 Secure Firewall 마이그레이션 툴과 같은 폴더에 저장됩니다.

단계 **1** Secure Firewall 마이그레이션 툴을 배치한 폴더로 이동합니다.

단계 **2** 로그를 저장하려면 `log` 폴더를 잘라내거나 복사하여 다른 위치에 붙여 넣습니다.

단계 **3** 마이그레이션 전 보고서와 마이그레이션 후 보고서를 저장하려면 `resources` 폴더를 잘라내거나 복사하여 다른 위치에 붙여 넣습니다.

단계 **4** Secure Firewall 마이그레이션 툴을 배치한 폴더를 삭제합니다.

팁 로그 파일은 콘솔 창과 연결되어 있습니다. Secure Firewall 마이그레이션 툴의 콘솔 창이 열려 있으면 로그 파일과 폴더를 삭제할 수 없습니다.

샘플 마이그레이션: FDM 매니지드 디바이스를 Threat Defense 2100으로

참고 마이그레이션을 완료한 후 대상 디바이스에서 실행할 수 있는 테스트 계획을 생성합니다.

- 유지 보수 기간 작업별
- 유지 보수 기간 작업

유지 보수 기간 작업별

시작하기 전에

management center를 설치하고 구축했는지 확인합니다. 자세한 내용은 해당 Firepower Management Center 하드웨어 설치 가이드 및 해당 Firepower Management Center 시작 가이드를 참고하십시오.

단계 1 FDM 매니지드 구성을 가져오거나 FDM 매니지드 디바이스에 연결하여 구성을 가져옵니다.

단계 2 FDM 매니지드 디바이스 구성 파일을 검토합니다.

단계 3 네트워크에 Firepower 2100 Series 디바이스를 구축하고 인터페이스를 연결한 다음 어플라이언스의 전원을 켭니다.

자세한 내용은 Management Center를 사용하는 2100 시리즈용 Cisco Threat Defense 빠른 시작 가이드를 참고하십시오.

단계 4 management center에서 관리할 Firepower 2100 Series 디바이스를 등록합니다.

자세한 내용은 Management Center에 디바이스 추가를 참고하십시오.

단계 5 (선택 사항) 소스 FDM 매니지드 디바이스 구성에 포트 채널이 있는 경우 대상 Firepower 2100 Series 디바이스에서 포트 채널(EtherChannels)을 생성합니다.

자세한 내용은 EtherChannel 및 이중 인터페이스 구성을 참고하십시오.

단계 6 https://software.cisco.com/download/home/286306503/type에서 Secure Firewall 마이그레이션 툴의 최신 버전을 다운로드하여 실행합니다.

자세한 내용은 Cisco.com에서 Secure Firewall 마이그레이션 툴 다운로드, 3 페이지을 참고하십시오.

단계 7 Secure Firewall 마이그레이션 툴을 실행하고 대상 매개변수를 지정할 때 management center에 등록한 Firepower 2100 Series 디바이스를 선택하십시오.

자세한 내용은 Secure Firewall 마이그레이션 툴에 대한 대상 매개변수 지정, 16 페이지을 참고하십시오.

단계 8 FDM 매니지드 디바이스 인터페이스와 Threat Defense 인터페이스를 매핑합니다.

참고 Secure Firewall 마이그레이션 툴을 사용하면 FDM 매니지드 디바이스 인터페이스 유형을 Threat Defense 인터페이스 유형에 매핑할 수 있습니다.

예를 들어 FDM 매니지드 디바이스의 포트 채널을 Threat Defense의 물리적 인터페이스에 매핑할 수 있습니다.

자세한 내용은 FDM 매니지드 디바이스 구성과 Secure Firewall Device Manager Threat Defense 인터페이스 매핑을 참고하십시오.

단계 **9** 논리적 인터페이스를 보안 영역에 매핑하는 동안 **Auto-Create(**자동 생성**)**를 클릭하여 Secure Firewall 마이그레이션 툴이 새 보안 영역을 생성하도록 허용합니다. 기존 보안 영역을 사용하려면 FDM 매니지드 디바이스 논리적 인터페이스를 보안 영역에 수동으로 매핑합니다.

자세한 내용은 FDM 매니지드 디바이스 인터페이스를 보안 영역에 매핑을 참고하십시오.

단계 **10** 이 가이드의 지침에 따라 마이그레이션할 컨피그레이션을 순차적으로 검토 및 검증한 다음 컨피그레이션을 management center로 푸시합니다.

단계 **11** 마이그레이션 후 보고서를 검토하고 Threat Defense에 다른 컨피그레이션을 수동으로 설정하고 구축한 다음 마이그레이션을 완료합니다.

자세한 내용은 마이그레이션할 컨피그레이션 최적화, 검토 및 검증, 23 페이지를 참고하십시오.

단계 **12** 마이그레이션을 계획하는 동안 생성한 테스트 계획을 사용하여 Firepower 2100 Series 디바이스를 테스트합니다.

유지 보수 기간 작업

시작하기 전에

유지 보수 기간 전에 수행해야 하는 모든 작업을 완료했는지 확인합니다. 유지 보수 기간 작업별, 38 페이지의 내용을 참조하십시오.

단계 **1** SSH 콘솔을 통해 FDM 매니지드 디바이스에 연결하고 인터페이스 구성 모드로 전환합니다.

단계 **2** **shutdown** 명령을 사용하여 FDM 매니지드 디바이스 인터페이스를 셧다운합니다.

단계 **3** (선택 사항) management center에 액세스하고 Firepower 2100 Series 디바이스의 동적 라우팅을 구성합니다.

자세한 내용은 동적 라우팅을 참고하십시오.

단계 **4** 주변 스위칭 인프라에서 ARP(Address Resolution Protocol) 캐시를 지웁니다.

단계 **5** 주변 스위칭 인프라에서 Firepower 2100 Series 디바이스 인터페이스 IP 주소에 대한 기본 ping 테스트를 수행하여 액세스 가능한지 확인합니다.

단계 **6** 레이어 3 라우팅이 필요한 디바이스에서 Firepower 2100 Series 디바이스 인터페이스 IP 주소에 대한 기본 ping 테스트를 수행합니다.

단계 **7** Firepower 2100 Series 디바이스에 새 IP 주소를 할당하고 FDM 매니지드 디바이스에 할당된 IP 주소를 재사용하지 않는 경우 다음 단계를 수행합니다.

1. 이제 Firepower 2100 Series 디바이스 IP 주소를 가리키도록 IP 주소를 참조하는 모든 정적 경로를 업데이트합니다.

2. 라우팅 프로토콜을 사용하는 경우 인접한 라우터(neighbor router)에서 Firepower 2100 Series 디바이스 IP 주소가 예상 대상의 다음 홉으로 표시되는지 확인합니다.

단계 **8** Firepower 2100 디바이스에 대해 관리 management center 내에서 포괄적인 테스트 계획을 실행하고 로그를 모니터링합니다.