기본 설정 구성

Security Cloud Control는 명확하고 간결한 인터페이스를 통해 정책 관리에 대한 고유한 보기를 제공합니다. 다음은 Security Cloud Control를 처음 사용할 때 기본 사항을 다루는 항목입니다.

- Security Cloud Control 테넌트 생성, on page 1
- Security Cloud Control 대시보드, 3 페이지
- Security Cloud Control 테넌트 생성, on page 5
- Security Cloud Control 대시보드, 7 페이지
- Security Cloud Control에 대한 로그인 요구 사항, 8 페이지
- **Cisco Secure Cloud Sign On** ID 제공자로 마이그레이션, 10 페이지
- Security Cloud Control 테넌트 시작, on page 12
- Security Cloud Control 통합 페이지, 13 페이지
- Security Cloud Control 라이선스, 16 페이지
- **Security Cloud Control** 플랫폼 유지 관리 일정, 18 페이지
- 클라우드 제공 Firewall Management Center 유지 관리 일정, 19 페이지
- 개체 소개, on page 19
- 네트워크 주소 변환, 49 페이지
- NAT 규칙 처리 순서, on page 49
- 네트워크 주소 변환 마법사, on page 51
- NAT의 일반적인 사용 사례, 52 페이지

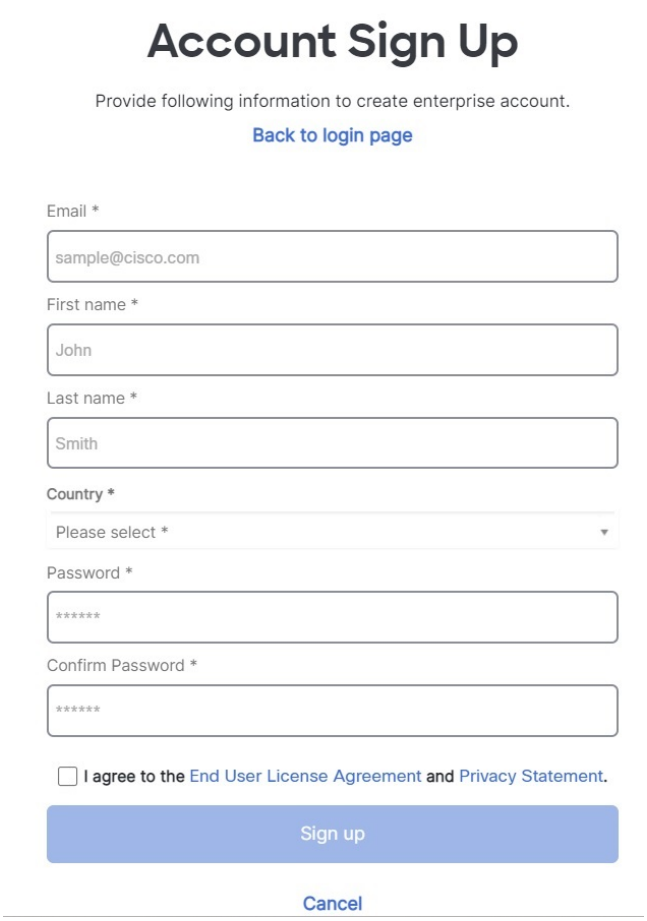
Security Cloud Control 테넌트 생성

디바이스를 온보딩하고 관리하기 위해 새 Security Cloud Control 테넌트를 프로비저닝할 수 있습니다. 온프레미스 방화벽 Management Center 버전 7.2 이상을 사용하고 이를 Cisco Security Cloud와 통합하려는 경우 통합 워크플로우의 일부로 Security Cloud Control 테넌트를 생성할 수도 있습니다.

절차

1. https://us.manage.security.cisco.com/provision로 진행합니다.
2. Security Cloud Control 테넌트를 프로비저닝하려는 지역을 선택하고 **Sign Up(**등록**)**을 클릭합니다.

3. **Security Cloud Sign On(**보안 클라우드 로그인**)** 페이지에서 자격 증명을 입력합니다.
4. Security Cloud Sign On 어카운트가 없고 새로 생성하려는 경우, **Sign up now(**지금 등록**)**를 클릭합니다.
   a. 어카운트를 생성하기 위한 정보를 입력하십시오.



다음은 몇 가지 팁입니다.

- **Email(**이메일**)**: Security Cloud Control에 로그인하는 데 사용할 이메일 주소를 입력합니다.
- **Password(**암호**)**: 강력한 암호를 입력하십시오.

   b. **Sign up(**등록하기**)**을 클릭합니다. Cisco는 등록한 주소로 확인 이메일을 보냅니다.
   c. 메일을 열고 메일 및 **Security Cloud Sign On(**보안 클라우드 로그인**)** 페이지에서 **Activate account(**어카운트 활성화**)**를 클릭합니다.
   d. 선택한 디바이스에서 Duo를 사용하여 다단계 인증을 구성하고 **Log in with Duo(Duo**로 로그인**)**을 클릭하고 **Finish(**마침**)**를 클릭합니다.

Note 휴대전화에 Duo Security 앱을 설치하는 것이 좋습니다. Duo 설치에 대한 질문은 Duo 2단계 인증 가이드: 등록 가이드를 참조하십시오.

5. 테넌트의 이름을 제공하고 **Create new account(**새 어카운트 생성**)**를 클릭합니다.
6. 선택한 지역에 새 Security Cloud Control 테넌트가 생성됩니다. 생성되는 Security Cloud Control 테넌트에 대한 세부 정보가 포함된 이메일도 받게 됩니다. 여러 Security Cloud Control 테넌트와 이미 연결되어 있는 경우 **Choose a tenant(**테넌트 선택**)** 페이지에서 로그인하기 위해 방금 생성한 테넌트를 선택합니다. 처음으로 새 Security Cloud Control 테넌트를 생성하는 경우 테넌트에 직접 로그인됩니다.

   Security Cloud Control 테넌트에 처음으로 로그인하는 방법에 대한 자세한 내용은 새 Security Cloud Control 테넌트에 최초 로그인을 참조하십시오.

   Security Cloud Control 테넌트 및 다양한 테넌트 설정 관리에 대한 자세한 내용은 테넌트 관리를 참조하십시오.

Security Cloud Control 테넌트를 정식 버전으로 업그레이드

Security Cloud Control의 무료 평가판을 사용 중인 경우 평가판 기간이 남은 기간 동안 Security Cloud Control의 무료 평가판을 사용 중이라는 배너가 계속 표시됩니다. 평가판 기간 중 언제든지 Security Cloud Control 테넌트를 정식 버전으로 업그레이드할 수 있습니다. 시스코 영업 담당자에게 문의하거나 시스코 영업팀에 연락하면 영업팀에서 대신 주문하고 세일즈 오더 번호를 받을 수 있습니다.

세일즈 오더 번호를 받으면 배너에서 정식 버전으로 업그레이드를 클릭하고 주문 번호를 입력하면 정식 버전의 Security Cloud Control를 사용할 수 있습니다.

Security Cloud Control 평가판 기간 연장 요청

평가판을 30일 동안 계속 사용하려면 **Request for an extension(**연장 요청**)**을 클릭합니다.

Security Cloud Control 대시보드

Security Cloud Control 대시보드는 다양한 범주에 걸쳐 조직 수준의 세부 정보를 모니터링하고 관리하기 위한 중앙 허브입니다. 로그인하면 중요한 인사이트와 보안 및 운영 효율성 최적화하기 위한 작업을 제공하는 맞춤형 대시보드에 액세스할 수 있습니다.

대시보드 사용자 맞춤화

표시되는 위젯을 맞춤 설정하여 대시보드를 특정 요구 사항에 맞게 조정합니다.

1. **Home** 페이지에서 **Customize(**맞춤화**)**를 클릭합니다.
2. 대시보드에 표시할 위젯을 선택하거나 선택을 해제합니다.
3. 위젯을 끌어다 놓아 원하는 대로 정렬할 수 있습니다.

상위 정보

이 섹션에서는 다양한 테넌트 수준 메트릭에 대한 상세한 인사이트를 제공합니다. 활성화된 경우 다음 위젯을 볼 수 있습니다.

- **Configuration States(**구성 상태**)**: 사용자의 디바이스에 설정된 구성과 Security Cloud Control에서 유지 관리하는 구성 간의 불일치를 나타냅니다. 이 비교를 통해 존재할 수 있는 불일치나 충돌을 식별하는 데 도움이 됩니다.

  자세한 내용은 디바이스 관리를 참조하십시오.

- **Change Log Management(**변경 로그 관리**)**: 정확한 운영 제어를 위해 변경 로그를 관리하는 데 도움이 됩니다. 위젯에 **Completed(**완료됨**)** 및 **Pending(**보류 중**)** 변경 로그가 표시됩니다.

  자세한 내용은 Change Logs(변경 로그)를 참조하십시오.

- **RA VPN Sessions(RA VPN** 세션**)**: 원격 액세스 VPN 세션을 모니터링할 수 있습니다.

  자세한 내용은 RA VPN 세션을 참조하십시오.

- **Overall Inventory(**전체 재고 목록**)**: 모든 디바이스의 상태를 모니터링할 수 있습니다. **Issues(**문제**)**, **Pending Actions(**보류 중인 작업**)**, **Other(**기타**)**, **Online(**온라인**)**으로 분류된 총 디바이스 수와 하드웨어 지원 기간이 가까워지거나 만료된 위젯의 총 수가 표시됩니다.

  자세한 내용은 모든 디바이스를 참조하십시오.

- **Site-to-Site VPN(**사이트 간 **VPN)**: 사이트 간 VPN 연결을 관리하고 평가하는 데 도움이 됩니다. 위젯에 총 VPN 터널 수와 **Active(**활성**)** 및 **Idle(**유휴**)**의 비율이 표시됩니다.

  자세한 내용은 사이트 간 VPN을 참조하십시오.

- 어카운트 및 자산:
  - 멀티 클라우드 어카운트 및 리소스를 효과적으로 추적하고 관리할 수 있습니다. 여기에서 Multicloud Defense 컨트롤러를 실행할 수 있습니다.
  - **+Add Account(+**어카운트 추가**)**를 클릭하여 새 어카운트을 추가합니다.

  자세한 내용은 Multicloud Defense Controller를 참조하십시오.

- **Top Risky Destinations(**상위 위험한 대상**)**: 액세스 권한이 부여된 상위 위험한 대상을 식별하고 모니터링하는 데 도움이 됩니다. 위젯은 애플리케이션 및 URL 범주를 나열하며, 지난 90일, 60일 또는 30일 동안의 데이터를 필터링할 수 있습니다. 허용된 트래픽(기본값)과 차단된 트래픽 사이에서 필터링할 수 있습니다.

- **Top Intrusion and Malware Events(**상위 침입 및 멀웨어 이벤트**)**: 상위 침입 및 멀웨어 이벤트를 모니터링하고 대응할 수 있습니다. 위젯은 침입 이벤트와 멀웨어이벤트를 표시하며, 지난 90일, 60일, 30일 동안의 데이터를 필터링할 수 있습니다. 허용된 이벤트(기본값)와 차단된 이벤트 사이에서 필터링할 수 있습니다.

발표

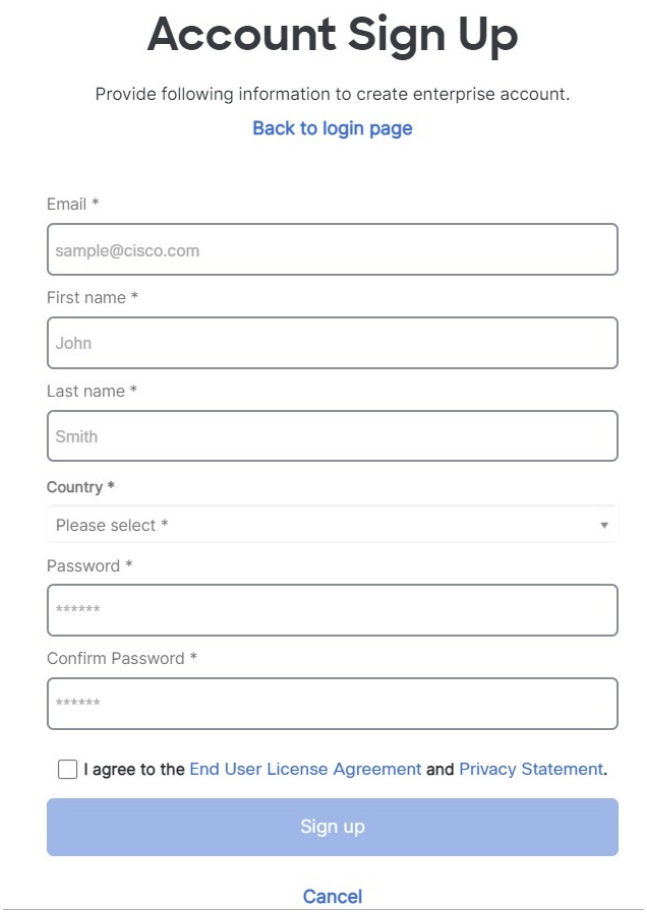
최신 Security Cloud Control 기능 및 업데이트를 보려면 알림 아이콘 클릭합니다. 목록에 있는 항목에 대한 추가 정보가 필요할 경우 관련 문서 링크가 제공됩니다.

Security Cloud Control 테넌트 생성

디바이스를 온보딩하고 관리하기 위해 새 Security Cloud Control 테넌트를 프로비저닝할 수 있습니다. 온프레미스 방화벽 Management Center 버전 7.2 이상을 사용하고 이를 Cisco Security Cloud와 통합하려는 경우 통합 워크플로우의 일부로 Security Cloud Control 테넌트를 생성할 수도 있습니다.

절차

1. https://us.manage.security.cisco.com/provision로 진행합니다.
2. Security Cloud Control 테넌트를 프로비저닝하려는 지역을 선택하고 **Sign Up(**등록**)**을 클릭합니다.
3. **Security Cloud Sign On(**보안 클라우드 로그인**)** 페이지에서 자격 증명을 입력합니다.
4. Security Cloud Sign On 어카운트가 없고 새로 생성하려는 경우, **Sign up now(**지금 등록**)**를 클릭합니다.
   a. 어카운트를 생성하기 위한 정보를 입력하십시오.



다음은 몇 가지 팁입니다.

- **Email(**이메일**)**: Security Cloud Control에 로그인하는 데 사용할 이메일 주소를 입력합니다.
- **Password(**암호**)**: 강력한 암호를 입력하십시오.

b. **Sign up(**등록하기**)**을 클릭합니다. Cisco는 등록한 주소로 확인 이메일을 보냅니다.

c. 메일을 열고 메일 및 **Security Cloud Sign On(**보안 클라우드 로그인**)** 페이지에서 **Activate account(**어카운트 활성화**)**를 클릭합니다.

d. 선택한 디바이스에서 Duo를 사용하여 다단계 인증을 구성하고 **Log in with Duo(Duo**로 로그인**)**을 클릭하고 **Finish(**마침**)**를 클릭합니다.

Note 휴대전화에 Duo Security 앱을 설치하는 것이 좋습니다. Duo 설치에 대한 질문은 Duo 2단계 인증 가이드: 등록 가이드를 참조하십시오.

5. 테넌트의 이름을 제공하고 **Create new account(**새 어카운트 생성**)**를 클릭합니다.
6. 선택한 지역에 새 Security Cloud Control 테넌트가 생성됩니다. 생성되는 Security Cloud Control 테넌트에 대한 세부 정보가 포함된 이메일도 받게 됩니다. 여러 Security Cloud Control 테넌트와 이미 연결되어 있는 경우 **Choose a tenant(**테넌트 선택**)** 페이지에서 로그인하기 위해 방금 생성한 테넌트를 선택합니다. 처음으로 새 Security Cloud Control 테넌트를 생성하는 경우 테넌트에 직접 로그인됩니다.

   Security Cloud Control 테넌트에 처음으로 로그인하는 방법에 대한 자세한 내용은 새 Security Cloud Control 테넌트에 최초 로그인을 참조하십시오.

   Security Cloud Control 테넌트 및 다양한 테넌트 설정 관리에 대한 자세한 내용은 테넌트 관리를 참조하십시오.

Security Cloud Control 테넌트를 정식 버전으로 업그레이드

Security Cloud Control의 무료 평가판을 사용 중인 경우 평가판 기간이 남은 기간 동안 Security Cloud Control의 무료 평가판을 사용 중이라는 배너가 계속 표시됩니다. 평가판 기간 중 언제든지 Security Cloud Control 테넌트를 정식 버전으로 업그레이드할 수 있습니다. 시스코 영업 담당자에게 문의하거나 시스코 영업팀에 연락하면 영업팀에서 대신 주문하고 세일즈 오더 번호를 받을 수 있습니다.

세일즈 오더 번호를 받으면 배너에서 정식 버전으로 업그레이드를 클릭하고 주문 번호를 입력하면 정식 버전의 Security Cloud Control를 사용할 수 있습니다.

Security Cloud Control 평가판 기간 연장 요청

평가판을 30일 동안 계속 사용하려면 **Request for an extension(**연장 요청**)**을 클릭합니다.

Security Cloud Control 대시보드

Security Cloud Control 대시보드는 다양한 범주에 걸쳐 조직 수준의 세부 정보을 모니터링하고 관리하기 위한 중앙 허브입니다. 로그인하면 중요한 인사이트와 보안 및 운영 효율성 최적화하기 위한 작업을 제공하는 맞춤형 대시보드에 액세스할 수 있습니다.

대시보드 사용자 맞춤화

표시되는 위젯을 맞춤 설정하여 대시보드를 특정 요구 사항에 맞게 조정합니다.

1. **Home** 페이지에서 **Customize(**맞춤화**)**를 클릭합니다.
2. 대시보드에 표시할 위젯을 선택하거나 선택을 해제합니다.
3. 위젯을 끌어다 놓아 원하는 대로 정렬할 수 있습니다.

상위 정보

이 섹션에서는 다양한 테넌트 수준 메트릭에 대한 상세한 인사이트를 제공합니다. 활성화된 경우 다음 위젯을 볼 수 있습니다.

- **Configuration States(**구성 상태**)**: 사용자의 디바이스에 설정된 구성과 Security Cloud Control에서 유지 관리하는 구성 간의 불일치를 나타냅니다. 이 비교를 통해 존재할 수 있는 불일치나 충돌을 식별하는 데 도움이 됩니다.

  자세한 내용은 디바이스 관리를 참조하십시오.

- **Change Log Management(**변경 로그 관리**)**: 정확한 운영 제어를 위해 변경 로그를 관리하는 데 도움이 됩니다. 위젯에 **Completed(**완료됨**)** 및 **Pending(**보류 중**)** 변경 로그가 표시됩니다.

  자세한 내용은 Change Logs(변경 로그)를 참조하십시오.

- **RA VPN Sessions(RA VPN** 세션**)**: 원격 액세스 VPN 세션을 모니터링할 수 있습니다.

  자세한 내용은 RA VPN 세션을 참조하십시오.

- **Overall Inventory(**전체 재고 목록**)**: 모든 디바이스의 상태를 모니터링할 수 있습니다. **Issues(**문제**)**, **Pending Actions(**보류 중인 작업**)**, **Other(**기타**)**, **Online(**온라인**)**으로 분류된 총 디바이스 수와 하드웨어 지원 기간이 가까워지거나 만료된 위젯의 총 수가 표시됩니다.

  자세한 내용은 모든 디바이스를 참조하십시오.

- **Site-to-Site VPN(**사이트 간 **VPN)**: 사이트 간 VPN 연결을 관리하고 평가하는 데 도움이 됩니다. 위젯에 총 VPN 터널 수와 **Active(**활성**)** 및 **Idle(**유휴**)**의 비율이 표시됩니다.

  자세한 내용은 사이트 간 VPN을 참조하십시오.

- 어카운트 및 자산:
  - 멀티 클라우드 어카운트 및 리소스를 효과적으로 추적하고 관리할 수 있습니다. 여기에서 Multicloud Defense 컨트롤러를 실행할 수 있습니다.
  - **+Add Account(+**어카운트 추가**)**를 클릭하여 새 어카운트을 추가합니다.

자세한 내용은 Multicloud Defense Controller를 참조하십시오.

- **Top Risky Destinations(**상위 위험한 대상**)**: 액세스 권한이 부여된 상위 위험한 대상을 식별하고 모니터링하는 데 도움이 됩니다. 위젯은 애플리케이션 및 URL 범주를 나열하며, 지난 90일, 60일 또는 30일 동안의 데이터를 필터링할 수 있습니다. 허용된 트래픽(기본값)과 차단된 트래픽 사이에서 필터링할 수 있습니다.
- **Top Intrusion and Malware Events(**상위 침입 및 멀웨어 이벤트**)**: 상위 침입 및 멀웨어 이벤트를 모니터링하고 대응할 수 있습니다. 위젯은 침입 이벤트와 멀웨어이벤트를 표시하며, 지난 90일, 60일, 30일 동안의 데이터를 필터링할 수 있습니다. 허용된 이벤트(기본값)와 차단된 이벤트 사이에서 필터링할 수 있습니다.

발표

최신 Security Cloud Control 기능 및 업데이트를 보려면 알림 아이콘 클릭합니다. 목록에 있는 항목에 대한 추가 정보가 필요할 경우 관련 문서 링크가 제공됩니다.

Security Cloud Control에 대한 로그인 요구 사항

Security Cloud Control에 로그인하려면 고객에게 SAML 2.0 호환 IdP(Identity Provider), 다단계 인증 제공자 및 Security Cloud Control의 사용자 레코드가 있는 어카운트가 필요합니다.

IdP 어카운트에는 사용자의 자격 증명이 포함되며 IdP는 이러한 자격 증명을 기반으로 사용자를 인증합니다. 다단계 인증은 ID 보안의 추가 레이어를 제공합니다. Security Cloud Control 사용자 레코드에는 주로 사용자 이름, 연결된 Security Cloud Control 테넌트 및 사용자의 역할이 포함됩니다. 사용자가 로그인하면 Security Cloud Control는 IdP의 사용자 ID를 Security Cloud Control의 테넌트에 있는 기존 사용자 레코드에 매핑하려고 시도합니다. Security Cloud Control가 일치 항목을 찾으면 사용자는 해당 테넌트에 로그인됩니다.

엔터프라이즈에 자체 SSO(Single Sign-On(단일 인증)) ID 제공자가 없는 경우 ID 제공자는 Security Cloud Sign On입니다. Security Cloud Sign On는 다단계 인증에 Duo를 사용합니다.

고객은 원하는 경우 자신의 IdP를 Security Cloud Control와 통합할 수 있습니다.

Security Cloud Control에 로그인하려면 먼저 Cisco Secure Cloud Sign-On에서 어카운트을 생성하고 Duo Security를 사용하여 MFA(Multi-Factor Authentication)를 구성하고 테넌트 최고 관리자가 Security Cloud Control 레코드를 생성하도록 해야 합니다.

2019년 10월 14일에 Security Cloud Control는 Cisco Secure Cloud Sign-On을 ID 제공자 및 MFA용 Duo로 사용하도록 기존의 모든 테넌트를 변환했습니다.

참고

- 자체 SSO(Single Sign-On) ID 제공자를 사용하여 Security Cloud Control에 로그인하는 경우 Cisco Secure Cloud Sign-On 및 Duo로의 전환이 영향을 미치지 않습니다. 고유한 로그인 솔루션을 계속 사용합니다.
- Security Cloud Control 무료 평가판을 사용 중인 경우 이 전환이 영향을 미쳤습니다.

Security Cloud Control 테넌트가 2019년 10월 14일 이후에 생성된 경우 새 Security Cloud Control 테넌트에 대한 초기 로그인, 9 페이지를 참조하십시오.

2019년 10월 14일 이전에 Security Cloud Control 테넌트가 존재했다면 Cisco Secure Cloud Sign On ID 제공자로 마이그레이션, 10 페이지를 참조하십시오.

새 **Security Cloud Control** 테넌트에 대한 초기 로그인

시작하기 전에

DUO Security 설치**.** 휴대전화에 Duo Security 앱을 설치하는 것이 좋습니다. Duo 설치에 대한 질문은 Duo 2단계 인증 가이드: 등록 가이드를 참조하십시오.

시간 동기화. 모바일 디바이스를 사용하여 일회용 비밀번호를 생성합니다. OTP는 시간을 기반으로 하므로 디바이스 시계를 실시간으로 동기화하는 것이 중요합니다. 디바이스 시계가 자동으로 또는 수동으로 올바른 시간으로 설정되었는지 확인합니다.

Security Cloud Control는 Cisco Secure Cloud Sign-On을 ID 제공자로 사용하며, MFA(multi-factor authentication)에는 Duo를 사용합니다. Cisco Security Cloud Sign On 어카운트가 없는 경우, 새 Security Cloud Control 테넌트를 생성하면 Security Cloud Sign On 프로비저닝 플로우에는 어카운트 생성 및 Duo를 사용한 MFA 구성 단계를 포함하여 다양한 단계가 포함됩니다, 새 테넌트 생성하려면 여기를 클릭합니다.

MFA는 사용자 ID를 보호하기 위해 추가 보안 레이어를 제공합니다. MFA 유형인 2단계 인증에서는 Security Cloud Control에 로그인하는 사용자의 ID를 확인하기 위해 두 가지 구성 요소 또는 요소가 필요합니다. 첫 번째 요소는 사용자 이름과 비밀번호이고, 두 번째 요소는 요청 시 생성되는 일회용 비밀번호(OTP)입니다.

중요 **2019**년 **10**월 **14**일 이전에 **Security Cloud Control** 테넌트가 존재했다면 이 문서 대신 Cisco Secure Cloud Sign On ID 제공자로 마이그레이션, 10 페이지을 사용하여 로그인 지침을 사용합니다.

다음 작업**?**

새 Cisco Secure Cloud Sign On 어카운트 생성 및 Duo 다단계 인증 구성를 진행합니다. 이는 4 단계 프로세스입니다. 4단계를 모두 완료해야 합니다.

다른 지역에서 **Security Cloud Control** 로그인

다음은 다른 AWS 지역에서 Security Cloud Control에 로그인하는 데 사용하는 URL입니다.

표 ***1: Security Cloud Control*** 다른 지역의 ***URL***

지역	**Security Cloud Control URL**
아시아 태평양 및 일본(APJ)	https://apj.manage.security.cisco.com

지역	**Security Cloud Control URL**
호주(AUS)	https://aus.manage.security.cisco.com
유럽, 중동 및 아프리카(EMEA)	https://eu.manage.security.cisco.com
인도(IN)	https://in.manage.security.cisco.com
미국(US)	https://us.manage.security.cisco.com

로그인 실패 문제 해결

실수로 잘못된 **Security Cloud Control** 지역에 로그인했기 때문에 로그인에 실패함

적절한 Security Cloud Control 지역에 로그인했는지 확인합니다. https://sign-on.security.cisco.com에 로그인하면 액세스할 지역을 선택할 수 있습니다.https://sign-on.security.cisco.com

로그인해야 하는 지역에 대한 자세한 내용은 다른 지역에서 Security Cloud Control 로그인, 9 페이지을 참조하십시오.

Cisco Secure Cloud Sign On ID 제공자로 마이그레이션

2019년 10월 14일, Security Cloud Control는 모든 테넌트를 MFA(multi-factor authentication)를 위한 ID 제공자 및 Duo로 Cisco Secure Cloud Sign-On으로 변환했습니다. **Security Cloud Control**에 로그인하려면 먼저 **Cisco Secure Sign-On**에서 어카운트를 활성화하고 **Duo**를 사용하여 **MFA**를 구성해야 합니다.

Security Cloud Control에는 사용자 ID를 보호하기 위해 추가 보안 레이어를 제공하는 MFA가 필요합니다. MFA 유형인 2단계 인증에서는 Security Cloud Control에 로그인하는 사용자의 ID를 확인하기 위해 두 가지 구성 요소 또는 요소가 필요합니다. 첫 번째 요소는 사용자 이름과 비밀번호이고, 두 번째 요소는 요청 시 생성되는 일회용 비밀번호(OTP)입니다.

참고

- 자체 SSO(Single Sign-On) ID 제공자를 사용하여 Security Cloud Control에 로그인하는 경우 Cisco Secure Cloud Sign-On 및 Duo로의 전환이 영향을 미치지 않습니다. 고유한 로그인 솔루션을 계속 사용합니다.
- Security Cloud Control 무료 평가판을 사용 중인 경우 이 전환이 적용됩니다.
- **Security Cloud Control** 테넌트가 **2019**년 **10**월 **14**일 이후에 생성된 경우 이 문서 대신 새 Security Cloud Control 테넌트에 대한 초기 로그인, 9 페이지에서 로그인 지침을 참조하십시오.

시작하기 전에

마이그레이션하기 전에 다음 단계를 수행하는 것이 좋습니다.

- **DUO Security** 설치**.** 휴대전화에 Duo Security 앱을 설치하는 것이 좋습니다. Duo 설치에 대한 질문은 Duo 2단계 인증 가이드: 등록 가이드를 참조하십시오.
- 시간 동기화. 모바일 디바이스를 사용하여 일회용 비밀번호를 생성합니다. OTP는 시간을 기반으로 하므로 디바이스 시계를 실시간으로 동기화하는 것이 중요합니다. 디바이스 시계가 자동으로 또는 수동으로 올바른 시간으로 설정되었는지 확인합니다.
- 새 Cisco Secure Cloud Sign On 어카운트 생성 및 Duo 다단계 인증 구성 이는 4 단계 프로세스입니다. 4단계를 모두 완료해야 합니다.

마이그레이션 후 로그인 실패 문제 해결

잘못된 사용자 이름 또는 암호로 인해 **Security Cloud Control**에 로그인하지 못함

해결 방법 Security Cloud Control에 로그인하려고 할 때 사용자 이름 및 비밀번호가 올바른 데도 로그인이 실패하는 것을 알고 있거나, "비밀번호를 잊음"를 시도하여 사용 가능한 비밀번호를 복원할 수 없는 경우, 새 Cisco Secure Cloud Sign-On 어카운트을 사용하려면 의 지침에 따라 새 Cisco Secure Cloud Sign-On 어카운트에 등록해야 합니다. 새 Cisco Security Cloud Sign On 어카운트을 등록해야 합니다.

해결 방법 참조: 새 Cisco Secure Cloud Sign On 어카운트 생성 및 Duo 다단계 인증 구성.

Cisco Secure Cloud Sign-On 대시보드 로그인에 성공했지만 **Security Cloud Control**를 실행할 수 없음

해결 방법 Security Cloud Control 테넌트와 다른 사용자 이름으로 Cisco Secure Cloud Sign-On 어카운트를 만들었을 수 있습니다. Security Cloud Control와 Cisco Secure Sign-On 간의 사용자 정보를 표준화하려면 Cisco TAC(Technical Assistance Center)에 문의하십시오.

저장된 북마크를 사용한 로그인 실패

해결 방법 브라우저에 저장한 이전 북마크를 사용하여 로그인을 시도했을 수 있습니다. 북마크는 https://cdo.onelogin.com을 가리킬 수 있습니다.

해결 방법 https://sign-on.security.cisco.com에 로그인합니다.

- 해결 방법 아직 Cisco Secure Sign-On 어카운트을 생성하지 않은 경우 어카운트을 생성합니다.
- 해결 방법 새 Secure Sign-On 어카운트를 만든 경우 대시보드에서 테넌트가 만들어진 지역에 해당하는 Security Cloud Control 타일을 클릭합니다.
  - 해결 방법 Security Cloud Control APJ
  - 해결 방법 Security Cloud Control 호주
  - 해결 방법 Security Cloud Control EU
  - 해결 방법 Security Cloud Control 인도
  - 해결 방법 Security Cloud Control US
- 해결 방법 https://sign-on.security.cisco.com를 가리키도록 즐겨찾기를 업데이트합니다.

Security Cloud Control 테넌트 시작

Procedure

단계 **1** Cisco Secure Cloud Sign-on 대시보드에서 해당 지역의 해당 Security Cloud Control 버튼을 클릭합니다.

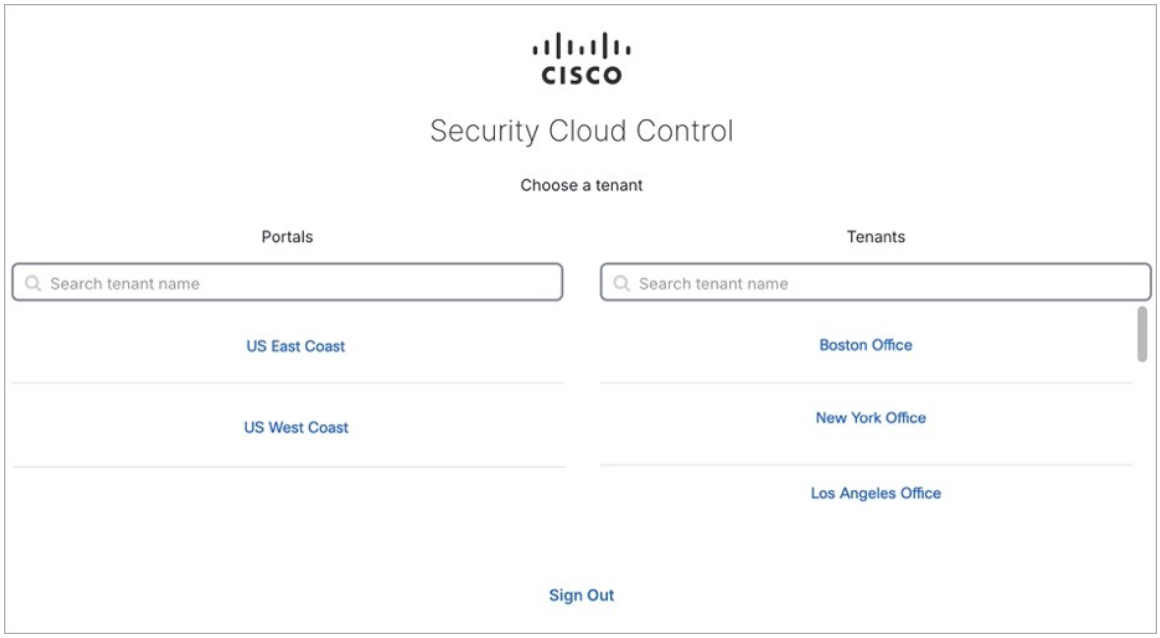
단계 **2** 두 인증자를 모두 설정한 경우 인증자 로고를 클릭하여 Duo Security 또는 Google Authenticator를 선택합니다.

- 기존 테넌트에 사용자 레코드가 이미 있는 경우 해당 테넌트에 로그인됩니다.
- 이미 여러 포털에 사용자 레코드가 있는 경우 연결할 포털을 선택할 수 있습니다.
- 여러 테넌트에 대한 사용자 레코드가 이미 있는 경우 연결할 Security Cloud Control 테넌트를 선택할 수 있습니다.
- 기존 테넌트에 대한 사용자 레코드가 아직 없는 경우 Security Cloud Control에 대해 자세히 알아보거나 평가판 테넌트를 요청할 수 있습니다.

포털 보기는 여러 테넌트에서 통합된 정보를 검색하고 표시합니다.

자세한 내용은 MSSP 포털를 참조하십시오.

테넌트 보기에는 사용자 레코드가 있는 여러 테넌트가 표시됩니다.

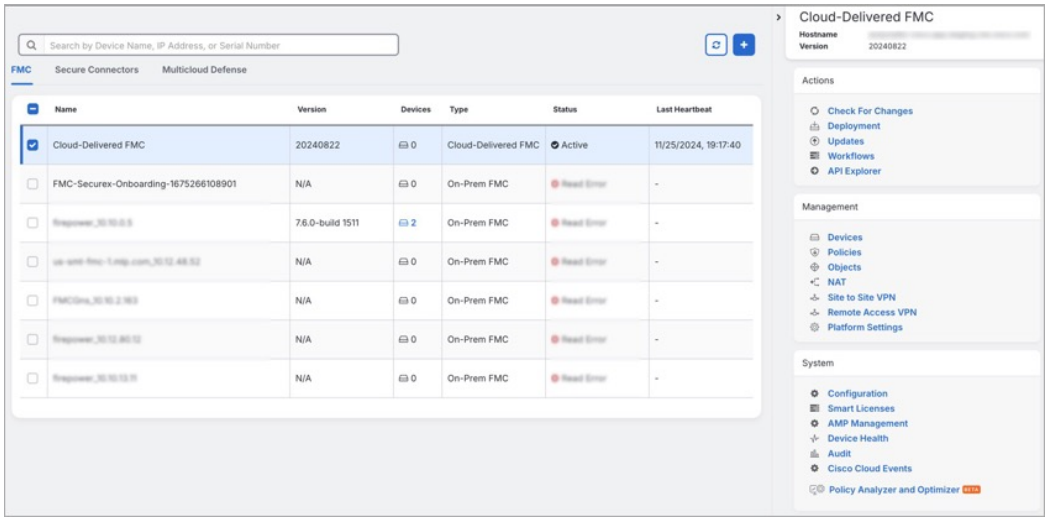


Security Cloud Control 통합 페이지

Integration(통합**)** 페이지에는 Firewall Management Center가 관리하는 Security Cloud Control 목록을 표시합니다. **FMC** 탭을 선택하면 Security Cloud Control 어카운트에 연결된 클라우드 제공 Firewall Management Center 및 Security Cloud Control에 온보딩된 모든 온프레미스 방화벽 Management Center가 나열됩니다. 이러한 온프레미스 Management Center에서 관리하는 디바이스는 **Security Devices(**보안 디바이스**)** 페이지에 나열됩니다. **Integration(**통합**)** 페이지의 **Secure Connector(**보안 커넥터**)** 탭 아래에도 보안 커넥터가 나열됩니다.

파란색 플러스 아이콘( )을 클릭하여 **FMC** 탭을 클릭하고 온프레미스 방화벽 Management Center를 온보딩한 후 오른쪽 창의 옵션을 사용하여 디바이스 작업을 수행할 수 있습니다. 디바이스의 버전, Management Center에서 관리하는 디바이스의 수, 디바이스 유형, 디바이스 동기화 상태 등의 디바이스 정보도 확인할 수 있습니다. 매니지드 디바이스 아이콘을 클릭하면 **Security Devices(**보안 디바이스**)** 페이지로 이동하며, 이 페이지에는 선택된 온프레미스 방화벽 Management Center에서 관리하는 디바이스가 자동으로 필터링되어 표시됩니다. **Integration(**통합**)** 페이지에서는 하나 이상의 온프레미스 방화벽 Management Center를 동시에 선택하여 Management Center 그룹에 대한 작업을 한 번에 수행할 수 있습니다. 클라우드 제공 Firewall Management Center가 선택된 상태에서는 온프레미스 방화벽 Management Center를 선택할 수 없습니다. 새 보안 커넥터를 추가하거나 기존 보안 커넥터에 대해 작업을 수행하려면 **Secure Connector(**보안 커넥터**)** 탭을 선택하고 를 클릭합니다.

왼쪽 창에서 **Administration(**관리**)** > **Firewall Management Center**를 클릭합니다.



클라우드 제공 Firewall Management Center의 경우 통합 페이지에 다음 정보가 표시됩니다.

- 클라우드 제공 Firewall Management Center가 테넌트에 구축되지 않은 경우, **Enable Cloud-Delivered FMC(**클라우드 제공 **FMC** 활성화**)**를 클릭합니다. 자세한 내용은 Security Cloud Control테넌트에서 클라우드 제공 Firewall Management Center 활성화를 참조하십시오.
- 클라우드 제공 Firewall Management Center에 구축된 Secure Firewall Threat Defense 디바이스 수.
- Security Cloud Control 및 클라우드 제공 Firewall Management Center 페이지 간의 연결 상태.

- 클라우드 제공 Firewall Management Center의 마지막 하트비트. 이는 클라우드 제공 Firewall Management Center 자체의 상태와 여기에서 관리하는 디바이스 수가 이 페이지의 테이블과 마지막으로 동기화된 것을 나타냅니다.
- 선택한 클라우드 제공 Firewall Management Center의 호스트 이름.

Cloud-Delivered FMC(클라우드 제공 **FMC)**를 선택하고 **Actions(**작업**)**, **Management(**관리**)** 또는 **Settings**(설정) 창의 링크를 사용하여 클릭한 링크와 연결된 구성 작업을 수행할 수 있는 클라우드 제공 Firewall Management Center사용자 인터페이스를 엽니다.

Actions(작업**)**:

- **Check For Changes(**변경 사항 확인**)**: 테이블의 디바이스 수 및 상태 정보가 이 페이지와 클라우드 제공 Firewall Management Center가 마지막으로 동기화되었을 때 사용 가능한 정보로 업데이트됩니다. 동기화는 10분마다 이루어집니다.
- **Deployment(**구축**)**: 클라우드 제공 Firewall Management Center의 디바이스 구성 구축 페이지로 이동합니다. 구성 변경 사항 구축을 참조하십시오.
- 워크플로우: 디바이스와 통신할 때 Security Cloud Control가 실행하는 모든 프로세스를 모니터링할 수 있는 워크플로우 페이지로 이동합니다. 워크플로우 페이지를 참조하십시오.
- **API Explorer**: 클라우드 제공 Firewall Management Center REST API를 나열하는 페이지로 이동합니다. Secure Firewall Management Center REST API 가이드를 참조하십시오.
- **Unified Events(**통합 이벤트**)**: 연결, 침입, 파일, 멀웨어 및 보안 관련 연결 이벤트를 비롯한 다양한 방화벽 이벤트를 단일 화면으로 볼 수 있는 클라우드 제공 Firewall Management Center 포털의 **Unified Events(**통합 이벤트**)** 페이지로 이동합니다. 통합 이벤트에 대한 자세한 내용은 Unified Events(통합 이벤트)를 참조하십시오.

참고 통합 이벤트 기능을 사용하려면 활성화가 필요합니다. 기능을 아직 활성화하지 않은 경우 시스코 영업 담당자에게 문의하여 활성화하십시오.

Management(관리**)**:

- **Devices(**디바이스**)**: 클라우드 제공 Firewall Management Center 포털의 Firewall Threat Defense 디바이스 목록 페이지로 이동합니다. 디바이스 구성을 참조하십시오.
- **Policies(**정책**)**: 시스템에서 제공한 액세스 제어 정책을 편집하고 사용자 정의 액세스 제어 정책을 생성할 수 있는 클라우드 제공 Firewall Management Center 포털의 정책 페이지로 이동합니다. 액세스 제어 정책 관리를 참조하십시오.
- **Objects(**개체**)**: 재사용 가능한 개체를 관리할 수 있는 클라우드 제공 Firewall Management Center 포털의 정책 페이지로 이동합니다. 개체 관리를 참조하십시오.
- **NAT**: Firewall Threat Defense 디바이스에 대한 네트워크 주소 변환 정책을 구성할 수 있는 클라우드 제공 Firewall Management Center 포털의 정책 페이지로 이동합니다. NAT 정책 관리를 참조하십시오.

- **Site to Site VPN(**사이트 간 **VPN)**: 두 사이트 간에 사이트 간 VPN 정책을 구성할 수 있는 클라우드 제공 Firewall Management Center 포털의 사이트 간 VPN 대시보드 페이지로 이동합니다. 사이트 간 VPN을 참조하십시오.
- **Remote Access VPN(**원격 액세스 **VPN)**: 원격 액세스 VPN을 구성할 수 있는 클라우드 제공 Firewall Management Center 포털의 원격 액세스 VPN 대시보드 페이지로 이동합니다. 원격 액세스 VPN을 참조하십시오.
- **Platform Settings(**플랫폼 설정**)**: 값을 여러 디바이스 간에 공유하려고 할 수 있는 비 관련 기능의 범위를 구성할 수 있는 클라우드 제공 Firewall Management Center 포털의 플랫폼 설정 페이지로 이동합니다. 플랫폼 설정을 참조하십시오.

System(시스템**)**:

- **Configuration(**구성**)**: 시스템 구성 설정을 구성할 수 있는 클라우드 제공 Firewall Management Center 포털의 시스템 구성 설정 페이지로 이동합니다. 시스템 구성을 참조하십시오.
- **Smart Licenses(**스마트 라이선스**)**: 디바이스에 라이선스를 할당할 수 있는 클라우드 제공 Firewall Management Center 포털의 스마트 라이선스 페이지로 이동합니다. 디바이스에 라이선스 할당을 참조하십시오.
- **AMP Management(AMP** 관리**)**: 시스템이 네트워크에서 멀웨어를 탐지하고 차단하는 데 사용하는 인텔리전스를 제공하는 클라우드 제공 Firewall Management Center 포털의 AMP 관리 페이지로 이동합니다. 멀웨어 차단을 위한 클라우드 연결을 참조하십시오.
- **Device Health(**디바이스 상태**)**: 다양한 상태 표시기를 추적하고 시스템의 하드웨어 및 소프트웨어가 올바르게 작동하는지 추적하는 클라우드 제공 Firewall Management Center 포털의 상태 모니터링 페이지로 이동합니다. 상태 모니터링 정보를 참조하십시오.
- **Audit(**감사**)**: 사용자와 웹 인터페이스의 각 상호 작용에 대해 생성된 감사 레코드를 표시할 수 있는 클라우드 제공 Firewall Management Center 포털의 감사 로그 페이지로 이동합니다.
- **Cisco Cloud Events(Cisco Cloud** 이벤트**)**: SAL(SaaS)에 이벤트를 직접 전송하도록 클라우드 제공 Firewall Management Center을(를) 구성할 수 있는 Security Cloud Control 포털의 Cisco Cloud 이벤트 구성 페이지로 이동합니다. SAL(SaaS)로 이벤트 전송을 참조하십시오.

클라우드 제공 Firewall Management Center 페이지가 열리면 파란색 물음표 버튼을 클릭하고 **Page-level Help(**페이지 수준 도움말**)**를 선택하여 현재 페이지와 수행 가능한 추가 작업에 대해 자세히 알아볼 수 있습니다.

별도의 탭에서 **Security Cloud Control** 및 클라우드 제공 **Firewall Management Center** 애플리케이션 열기 지원

클라우드 제공 Firewall Management Center에서 Firewall Threat Defense 디바이스 또는 개체를 구성할 때 추가 브라우저 탭에서 해당 구성 페이지를 열면 로그아웃하지 않고도 Security Cloud Control 및 클라우드 제공 Firewall Management Center 포털에서 동시에 작업할 수 있습니다.

예를 들어, 클라우드 제공 Firewall Management Center에서 개체를 생성하고 동시에 보안 정책에서 생성된 Security Cloud Control의 이벤트 로그를 모니터링할 수 있습니다.

이 기능은 클라우드 제공 Firewall Management Center 포털로 이동하는 모든 Security Cloud Control 링크에서 사용할 수 있습니다. 새 탭에서 클라우드 제공 Firewall Management Center 포털을 여는 방법:

Security Cloud Control 포털에서 Ctrl(Windows) 또는 Command(Mac) 버튼을 누른 상태로 해당 링크를 클릭합니다.

참고 한 번 클릭하면 동일한 탭에서 클라우드 제공 Firewall Management Center 페이지가 열립니다.

다음은 새 탭에서 클라우드 제공 Firewall Management Center 포털 페이지를 여는 몇 가지 예입니다.

- **Administration(**관리**)** > **Firewall Management Center**를 선택하고 **Cloud-Delivered FMC(**클라우드 제공 **FMC)**를 선택합니다. 오른쪽 창에서 Ctrl(Windows) 또는 Command(Mac) 버튼을 누른 상태로 액세스하려는 페이지를 클릭합니다.
- **Objects(**개체**)** > **Other FTD Objects(**기타 **FTD** 개체**)**를 선택합니다.
- Security Cloud Control 페이지 오른쪽 상단 모서리에 있는 검색 아이콘을 클릭하고 표시되는 검색 필드에 검색 문자열을 입력합니다.

  검색 결과에서 Ctrl(Windows) 또는 Command(Mac) 버튼을 누른 상태로 화살표 아이콘을 클릭합니다.
- **Dashboard(**대시보드**)** > **Quick Actions(**빠른 작업**)**를 선택합니다. **Ctrl**(Windows) 또는 **Command**(Mac) 버튼을 누른 상태에서 Manage FTD Policies(FTD 정책 관리) 또는 Manage FTD Objects(FTD 개체 관리)를 클릭합니다.

참고 새 Security Cloud Control 테넌트로 전환하면 새 탭에서 이미 열린 해당 클라우드 제공 Firewall Management Center 포털이 로그아웃됩니다.

관련 주제

- Security Cloud Control을 사용하여 온프레미스 Firewall Management Center 관리
- 온프레미스 Firewall Management Center 온보딩
- Security Cloud Control 테넌트에 대한 클라우드 제공 Firewall Management Center 요청
- Secure Device Connector
- 보안 이벤트 커넥터

Security Cloud Control 라이선스

Security Cloud Control는 조직 자격에 대한 기본 구독과 디바이스 관리를 위한 디바이스 라이선스가 필요합니다. 필요한 테넌트 수에 따라 하나 이상의 Security Cloud Control 기본 구독을 구입하고 디바이스 모델 번호 및 수량에 따라 디바이스 라이선스를 구입할 수 있습니다. 즉, 기본 구독을 구매하면

Security Cloud Control 조직이 제공되며 Security Cloud Control을 사용하여 관리하기로 선택한 모든 디바이스에 대해 별도의 디바이스 라이선스가 필요합니다.

Security Cloud Control에서 디바이스를 온보딩하고 관리하려면, 관리하려는 디바이스에 따라 기본 구독 및 디바이스별 기간 기반 구독을 구매해야 합니다.

구독

Security Cloud Control 구독은 기간 기반입니다.

- 기본- 1년, 3년 및 5년 동안의 구독을 제공하고 Security Cloud Control 조직에 액세스하고 적절하게 라이선스가 부여된 디바이스를 온보딩할 수 있는 권한을 제공합니다.
- 디바이스 라이선스 - 관리하기로 선택한 모든 지원 디바이스에 대해 1년, 3년 및 5년 구독을 제공합니다. 예를 들어 Cisco Firepower 1010 디바이스에 대한 3년 소프트웨어 구독을 구매한 경우, 3년 동안 Security Cloud Control을 사용하여 Cisco Firepower 1010 디바이스를 관리하도록 선택할 수 있습니다.

Security Cloud Control가 지원하는 Cisco 보안 디바이스에 대한 자세한 내용은 Security Cloud Control에서 지원하는 소프트웨어 및 하드웨어를 참조하십시오.

참고 Catalyst SD-WAN에는 추가 라이선스가 필요하지 않습니다. DNA 또는 WAN Essentials 라이선스를 사용하는 고객은 Security Cloud Control와 통합할 수 있습니다.

중요 Security Cloud Control에서 고가용성 디바이스 쌍을 관리하기 위해 두 개의 별도 디바이스 라이선스가 필요하지 않습니다. ASA(고가용성 쌍이 있는 경우, Security Cloud Control는 고가용성 디바이스 쌍을 하나의 단일 디바이스로 간주하므로 하나의 디바이스 라이선스를 구입하는 것으로 충분합니다.

참고 Cisco 스마트 라이선스 포털을 통해 Security Cloud Control 라이선스를 관리할 수 없습니다.

소프트웨어 구독 지원

Security Cloud Control 기본 구독에는 구독 기간 동안 유효한 소프트웨어 구독 지원이 포함되며 추가 비용 없이 소프트웨어 업데이트, 주요 업그레이드 및 Cisco TAC(Technical Assistance Center)에 대한 액세스를 제공합니다. 소프트웨어 지원이 기본적으로 선택되어 있지만 요구 사항에 따라 Security Cloud Control 솔루션 지원을 활용할 수도 있습니다.

클라우드 제공 **Firewall Management Center** 및 **Threat Defense** 라이선스

Security Cloud Control에서 클라우드 제공 Firewall Management Center를 사용하기 위해 별도의 라이선스를 구입할 필요가 없습니다. Security Cloud Control 테넌트의 기본 구독에는 클라우드 제공 Firewall Management Center에 대한 비용이 포함됩니다.

클라우드 제공 **Firewall Management Center** 평가 라이선스

클라우드 제공 Firewall Management Center은 90일 평가판 라이선스가 제공됩니다. 평가 기간이 경과한 후에도 Firewall Threat Defense 디바이스를 클라우드 제공 Firewall Management Center에 계속 온보딩할 수 있습니다. 단, 수동으로 트리거되거나 예약된 다른 모든 구축은 클라우드 제공 Firewall Management Center을 CSSM(Cisco Smart Software Manager)에 등록할 때까지 차단됩니다. 평가판 라이선스가 만료되면 Security Cloud Control이 알림 창의 알림을 통해 사용자에게 알립니다.

CSSM에 등록한 후 사용하고자 하는 기능에 필요한 라이선스를 구매하는 것을 권장합니다. 라이선스를 구매하면 클라우드 제공 Firewall Management Center이 컴플라이언스 위반 상태가 되지 않도록 합니다.

클라우드 제공 Firewall Management Center을 CSSM에 등록하는 방법에 대한 자세한 내용은 Management Center를 Smart Software Manager에 등록을 참조하십시오.

Security Cloud Control 테넌트에서 프로비저닝된 클라우드 제공 Firewall Management Center를 가져오는 방법을 알아보려면 Security Cloud Control 테넌트용 클라우드 제공 Firewall Management Center 요청을 참조하십시오.

참고 클라우드 제공 Firewall Management Center는 에어갭 네트워크의 디바이스에 대한 특정 라이선스 예약(SLR)을 지원하지 않습니다.

클라우드 제공 **Firewall Management Center**용 **Threat Defense** 라이선스

클라우드 제공 Firewall Management Center에서 관리하는 각 Secure Firewall Threat Defense 디바이스에 대해 개별 라이선스가 필요합니다. 자세한 내용은 *Security Cloud Control*에서 클라우드 제공 *Firewall Management Center*로 *Firewall Threat Defense* 관리에서 라이선싱을 참조하십시오.

Security Cloud Control가 클라우드 제공 Firewall Management Center으로 마이그레이션된 디바이스에 대한 라이선스를 처리하는 방법을 알아보려면 Management Center에서 Cloud로 Threat Defense 마이그레이션을 참조하십시오.

참고 Secure Firewall 버전 7.6.0의 평가 모드용 Talos 인증서가 2025년 3월 31일에 만료될 예정입니다. 이 날짜 이후로 평가 모드에서 Talos 호스팅 서비스(특히 웹 평판/범주 조회 관련 서비스)에 대한 액세스가 중단됩니다.

Security Cloud Control 플랫폼 유지 관리 일정

Security Cloud Control은 새로운 기능과 품질 개선으로 매주 플랫폼을 업데이트합니다. 이 일정에 따라 업데이트가 3시간 동안 이루어집니다.

요일	시간 **(24**시간제**, UTC)**
목요일	09:00 UTC - 12:00 UTC

이 유지 관리 기간 동안 조직에 계속 액세스할 수 있으며 클라우드 제공 Firewall Management Center 또는 Multicloud Defense 컨트롤러가 있는 경우, 해당 플랫폼에도 액세스할 수 있습니다. 또한 Security Cloud Control에 온보딩한 디바이스가 보안 정책을 계속 적용합니다.

참고

- 유지 관리 기간 동안 관리하는 디바이스에 구성 변경 사항을 구축하는 데 Security Cloud Control을 사용하지 않는 것이 좋습니다.
- Security Cloud Control과 통신이 중단되는 문제가 발생하면 유지보수 기간이 아니더라도 영향을 받는 모든 테넌트에게 최대한 신속하게 장애를 해결합니다.

클라우드 제공 **Firewall Management Center** 유지 관리 일정

테넌트에 구축된 클라우드 제공 Firewall Management Center을 보유한 고객은 Security Cloud Control가 클라우드 제공 Firewall Management Center 환경을 업데이트하기 약 1주일 전에 알림을 받습니다. 테넌트의 슈퍼 관리자 및 관리자 사용자에게는 이메일 알림이 전송됩니다. Security Cloud Control 는 또한 모든 사용자에게 향후 업데이트를 알리는 배너를 홈페이지에 표시합니다.

참고

- 유지 관리 기간 동안 관리하는 디바이스에 구성 변경 사항을 구축하는 데 클라우드 제공 Firewall Management Center을 사용하지 않는 것이 좋습니다.
- Security Cloud Control또는 클라우드 제공 Firewall Management Center과 통신이 중단되는 문제가 발생하면 유지보수 기간이 아니더라도 영향을 받는 모든 테넌트에게 최대한 신속하게 장애를 해결합니다.

개체 소개

개체는 하나 이상의 보안 정책에서 사용할 수 있는 정보의 컨테이너입니다. 개체를 사용하면 정책 일관성을 쉽게 유지할 수 있습니다. 단일 개체를 만들고 다른 정책을 사용하고 개체를 편집할 수 있으며 해당 변경 사항은 개체를 사용하는 모든 정책에 전파됩니다. 개체가 없는 경우 동일한 변경이 필요한 모든 정책을 개별적으로 수정해야 합니다.

디바이스를 온보딩하면, Security Cloud Control는 해당 디바이스에서 사용하는 모든 개체를 인식하고, 저장한 다음, **Objects(**개체**)** 페이지에 나열합니다. **Objects(**개체**)** 페이지에서 기존 개체를 편집하고 보안 정책에 사용할 새 개체를 생성할 수 있습니다.

Security Cloud Control은 여러 디바이스에서 사용되는 개체를 **shared object(**공유 개체**)**라고 부르고 **Objects(**개체**)** 페이지에서 이 배지로 식별합니다.

때때로 공유 개체는 일부 "문제"를 발생시키고 더 이상 여러 정책 또는 디바이스에서 완벽하게 공유되지 않습니다.

- **Duplicate objects(**중복 개체**)**는 이름은 다르지만 값은 같은 동일한 디바이스에 있는 두 개 이상의 개체입니다. 이러한 개체는 일반적으로 비슷한 용도로 사용되며 다른 정책에서 사용됩니다. 중복 개체는 다음 문제 아이콘로 식별됩니다.
- **Inconsistent objects(**일관성 없는 개체**)** 는 이름은 같지만 값이 다른 두 개 이상의 디바이스에 있는 개체입니다. 때로는 사용자가 동일한 이름과 콘텐츠로 다른 구성으로 개체를 생성하지만 시간이 지남에 따라 이러한 개체의 값이 달라져 불일치가 발생합니다. 일관성 없는 개체는 다음 문제 아이콘로 식별됩니다.
- 사용되지 않는 개체는 디바이스 구성에 존재하지만 다른 개체, 액세스 목록 또는 NAT 규칙에서 참조하지 않는 개체입니다. 사용되지 않는 개체는 다음 문제 아이콘로 식별됩니다.

규칙 또는 정책에서 즉시 사용할 개체를 생성할 수도 있습니다. 규칙 또는 정책과 연결되지 않은 개체를 생성할 수 있습니다. 규칙이나 정책에서 연결되지 않은 개체를 사용하는 경우, Security Cloud Control는 해당 개체의 복사본을 생성하고 해당 복사본을 사용합니다.

Objects(개체**)** 메뉴로 이동하거나 네트워크 정책의 세부 정보에서 확인하여 Security Cloud Control에 의해 관리되는 개체를 볼 수 있습니다.

Security Cloud Control은 한 위치에서 지원되는 디바이스 전체에 걸쳐 네트워크 및 서비스 개체를 관리할 수 있습니다. Security Cloud Control에서는 다음과 같은 방법으로 개체를 관리할 수 있습니다.

- 다양한 기준에 따라 모든 개체 https://securitydocs.cisco.com/api/v0/apps?appId=SccCdo&topic=cdo_object_filter를 검색하고 필터링할 수 있습니다.
- 디바이스에서 중복되거나, 사용되지 않거나, 일관성이 없는 개체를 찾고 이러한 개체 문제를 통합, 삭제 또는 해결하십시오.
- 연결되지 않은 개체를 찾아 사용하지 않는 경우 삭제합니다.
- 여러 디바이스에서 공통적인 공유 개체를 검색합니다.
- 변경 사항을 커밋하기 전에 일련의 정책 및 디바이스에 대한 개체 변경 사항의 영향을 평가합니다.
- 다양한 정책 및 디바이스와 개체 및 개체의 관계 집합을 비교합니다.
- Security Cloud Control에 온보딩된 후 디바이스에서 사용 중인 개체를 캡처합니다.

온보딩된 디바이스에서 개체를 생성, 편집 또는 읽는 데 문제가 있는 경우 자세한 내용은 문제 해결 Security Cloud Control 을 참조하십시오.

개체 유형

다음 표에서는 Security Cloud Control를 사용하여 디바이스에 대해 생성하고 관리할 수 있는 개체에 대해 설명합니다.

Table 2: 온프레미스 ***Secure Firewall Management Center*** 개체 유형

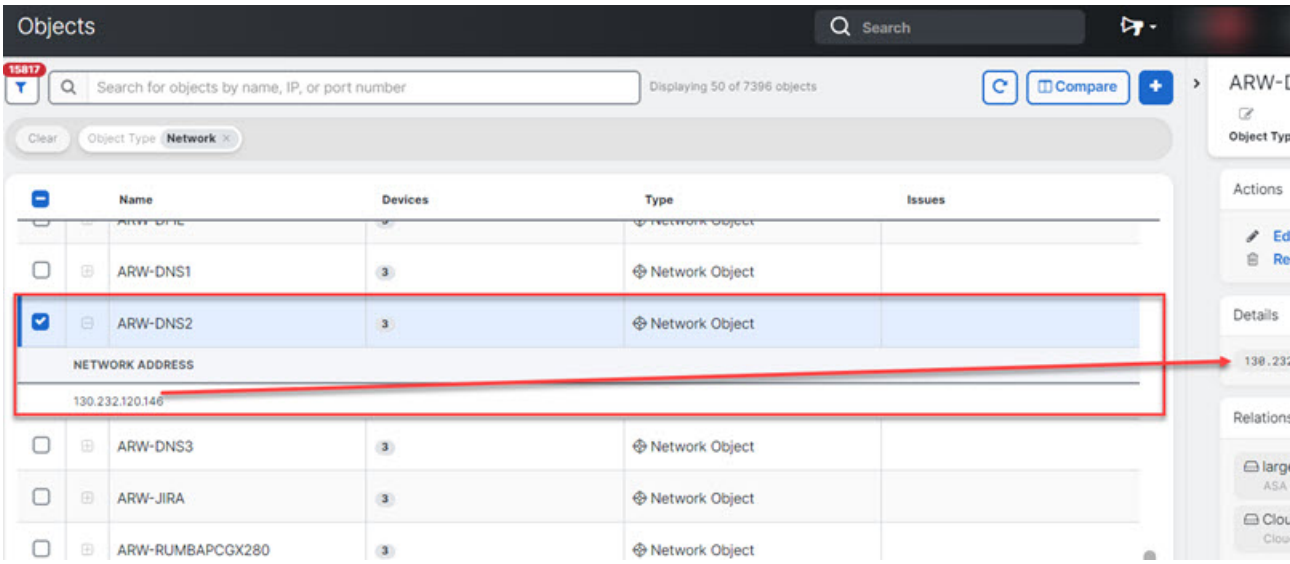
개체	설명
네트워크	네트워크 그룹과 네트워크 개체(네트워크 개체로 총칭함)는 호스트 또는 네트워크의 주소를 정의합니다.
서비스	서비스 개체, 서비스 그룹 및 포트 그룹은 TCP/IP 프로토콜 제품군의 일부로 간주되는 프로토콜 또는 포트를 포함하는 재사용 가능한 구성 요소입니다.

공유 개체

Security Cloud Control는 이름과 콘텐츠가 동일한 여러 디바이스의 개체인 공유 개체를 호출합니다. 공유 개체는 이 아이콘으로 식별됩니다.

Objects(개체**)** 페이지에서 공유 개체를 사용하면 한 곳에서 개체를 수정할 수 있으며 변경 사항은 해당 개체를 사용하는 다른 모든 정책에 영향을 미치므로 정책을 쉽게 유지 관리할 수 있습니다. 공유 개체가 없으면 동일한 변경이 필요한 모든 정책을 개별적으로 수정해야 합니다.

공유 개체를 볼 때 Security Cloud Control는 개체 테이블에 있는 개체의 내용을 표시합니다. 공유 개체는 정확히 동일한 내용을 갖습니다. Security Cloud Control는 세부 정보 창에서 개체 요소의 결합된 보기 또는 "평평한" 보기를 보여줍니다. 세부 정보 창에서 네트워크 요소는 간단한 목록으로 병합되며 명명된 개체와 직접 연결되지 않습니다.

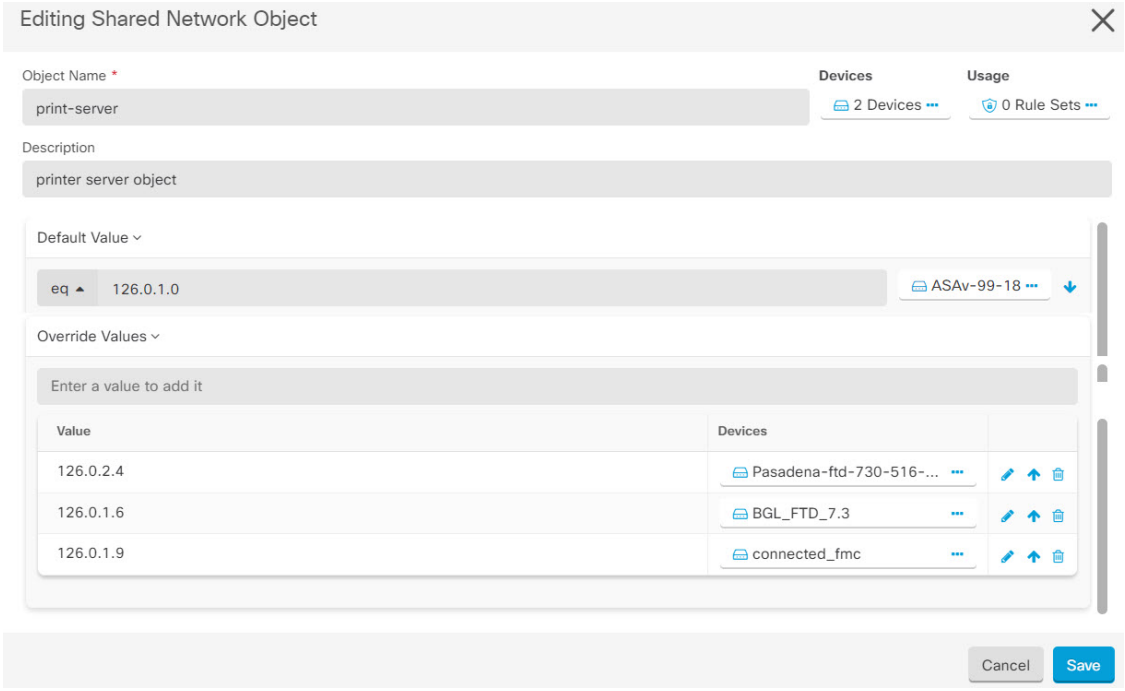


개체 재정의

개체 재정의는 특정 디바이스에서 공유 네트워크 객체의 값을 재정의할 수 있게 해줍니다. Security Cloud Control는 재정의 구성 시 지정한 디바이스에 해당하는 값을 사용합니다. 이름은 같지만 값이 다른 두 개 이상의 디바이스에 있는 개체에 대하여 Security Cloud Control는 이러한 값이 재정의되기 때문에 **Inconsistent objects(**일관성 없는 개체**)**로 식별하지 않습니다.

대부분의 디바이스에 대한 정의가 해당하는 개체를 생성하고 다른 정의가 필요한 일부 디바이스의 개체에 대한 특정 변경 사항을 지정하는 재정의를 사용할 수 있습니다. 모든 디바이스에 재정의가 필요한 개체를 생성할 수도 있습니다. 하지만 이 경우 모든 디바이스에 단일 정책을 생성할 수 있습니다. 개체 재정의는 필요한 경우 개별 디바이스의 정책을 바꾸지 않고도 디바이스 전반에 걸쳐 사용이 가능한 작은 공유 정책 집합을 생성하도록 합니다.

예를 들어 각 사무실에 .프린터 서버가 있고, 프린터 서버 개체인 `print-server`를 만든 시나리오를 생각해 보십시오. ACL에는 프린터 서버가 인터넷에 액세스하는 것을 거부하는 규칙이 있습니다. 프린터 서버 개체에는 한 사무실에서 다른 사무실로 변경하려는 기본값이 있습니다. 값이 다를 수 있지만 개체 재정의를 사용하고 규칙과 "프린터-서버" 개체를 모든 위치에서 일관되게 유지함으로써 이 작업을 수행할 수 있습니다.



Note 일관되지 않은 개체가 있는 경우 재정의를 통해 개체를 단일 공유 개체로 결합할 수 있습니다. 자세한 내용은 불일치 개체 문제 해결을 참조하십시오.

연결 해제된 개체

규칙 또는 정책에서 즉시 사용할 개체를 생성할 수 있습니다. 규칙이나 정책과 연결되지 않은 개체를 생성할 수도 있습니다. 규칙이나 정책에서 연결되지 않은 개체를 사용하는 경우, Security Cloud Control는 해당 개체의 복사본을 생성하고 해당 복사본을 사용합니다. 연결되지 않은 원래 개체는 야간 유지 관리 작업에 의해 삭제되거나 사용자가 삭제할 때까지 사용 가능한 개체 목록에 남아 있습니다.

개체와 연결된 규칙 또는 정책이 실수로 삭제된 경우 모든 구성이 손실되지 않도록 연결되지 않은 개체는 사본으로 Security Cloud Control에 남아 있습니다.

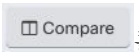
왼쪽 창 에서 **Objects(**개체**)** > 를 클릭하고 **Unassociated(**연결되지 않음**)** 체크 박스를 선택합니다.

개체 비교

Procedure

단계 **1** 왼쪽 창에서 **Objects(**개체**)**를 클릭하고 옵션을 선택합니다.

단계 **2** 페이지에서 개체를 필터링하여 비교하려는 개체를 찾습니다.

단계 **3** **Compare(**비교**)** 버튼 

를 클릭합니다.

단계 **4** 비교할 개체를 최대 3개까지 선택합니다.

단계 **5** 화면 하단에서 개체를 나란히 봅니다.

- 개체 세부 정보 제목 표시줄에서 위쪽 및 아래쪽 화살표를 클릭하면 개체 세부 정보를 더 많이 또는 더 적게 볼 수 있습니다.
- 세부 정보 및 관계 상자를 확장하거나 축소하여 더 많거나 적은 정보를 확인합니다.

단계 **6** (선택 사항) 관계 상자는 개체가 사용되는 방식을 보여줍니다. 디바이스 또는 정책과 연결될 수 있습니다. 개체가 디바이스와 연결된 경우 디바이스 이름을 클릭한 다음 **View Configuration(**구성 보기**)**을 클릭하여 디바이스 구성을 볼 수 있습니다. Security Cloud Control는 디바이스의 구성 파일을 표시하고 해당 개체에 대한 항목을 강조 표시합니다.

필터

Security Devices(보안 디바이스**)** 및 **Objects(**개체**)** 페이지에서 다양한 필터를 사용하여 원하는 디바이스 및 개체를 찾을 수 있습니다.

필터링하려면 Security Devices(보안 디바이스), Policies(정책) 및 Objects(개체) 탭의 왼쪽 창에서 
을 클릭합니다.

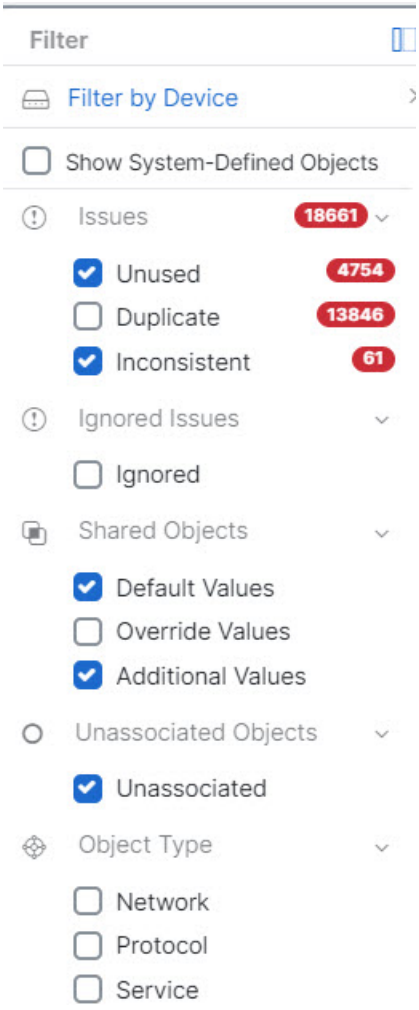
보안 디바이스 필터를 사용하면 디바이스 유형, 하드웨어 및 소프트웨어 버전, snort 버전, 구성 상태, 연결 상태, 충돌 탐지, 보안 디바이스 커넥터 및 레이블을 기준으로 필터링할 수 있습니다. 필터를 적용하여 선택한 디바이스 유형 탭 내에서 디바이스를 찾을 수 있습니다. 필터를 사용하여 선택한 디바이스 유형 탭 내에서 디바이스를 찾을 수 있습니다.

개체 필터를 사용하면 디바이스, 문제 유형, 공유 개체, 연결되지 않은 개체 및 개체 유형을 기준으로 필터링할 수 있습니다. 결과에 시스템 개체를 포함하거나 포함하지 않을 수 있습니다. 또한 검색 필드를 사용하여 필터 결과에서 특정 이름, IP 주소 또는 포트 번호를 포함하는 개체를 검색할 수 있습니다.

개체 유형 필터를 사용하면 네트워크 개체, 네트워크 그룹, URL 개체, URL 그룹, 서비스 개체, 서비스 그룹 등의 유형별로 개체를 필터링할 수 있습니다. 공유 개체 필터를 사용하면 기본값 또는 재정의 값이 있는 개체를 필터링할 수 있습니다.

디바이스 및 개체를 필터링할 때 검색 용어를 결합하여 몇 가지 잠재적 검색 전략을 생성하여 관련 결과를 찾을 수 있습니다.

다음 예제에서는 "문제(미사용 또는 일관성 없음) 및 공유 개체(기본값 또는 추가값 있음) 및 연결되지 않은 개체" 검색에 필터를 적용합니다.



개체 필터

필터링하려면 Objects(개체) 탭의 왼쪽 창에서 을(를) 클릭합니다.

- **Filter by Device(**디바이스별 필터**)**: 선택한 디바이스에 있는 개체를 볼 수 있도록 특정 디바이스를 선택할 수 있습니다.
- **Issues(**문제**)**: 사용하지 않거나 중복되고 일치하지 않는 개체를 선택하여 볼 수 있습니다.
- **Ignored Issues(**무시된 문제**)**: 불일치가 무시했던 모든 개체를 볼 수 있습니다.
- **Shared Objects(**공유 개체**)**: Security Cloud Control가 둘 이상의 디바이스에서 공유된 것으로 확인된 모든 개체를 볼 수 있습니다. 기본값만, 재정의 값 또는 둘 다를 사용하여 공유 개체를 보도록 선택할 수 있습니다.
- **Unassociated Objects(**연결되지 않은 개체**)**: 규칙이나 정책과 연결되지 않은 모든 개체를 볼 수 있습니다.

- **Object Type(**개체 유형**)**: 개체 유형을 선택하여 네트워크 개체, 네트워크 그룹, URL 개체, URL 그룹, 서비스 개체 및 서비스 그룹과 같이 선택한 유형의 개체만 표시할 수 있습니다.

하위 필터 – 각 기본 필터에는 선택 범위를 좁히기 위해 적용할 수 있는 하위 필터가 있습니다. 이러한 하위 필터는 네트워크, 서비스, 프로토콜 등의 개체 유형을 기반으로 합니다.

이 필터 표시줄에서 선택한 필터는 다음 기준과 일치하는 개체를 반환합니다.

* 두 디바이스 중 하나에 있는 개체. (디바이스를 지정하려면 **Filter by Device(**디바이스별 필터링**)**를 클릭합니다.) 및

* 일치하지 않는 개체 및

* 네트워크 개체 또는 서비스 개체 및

* 개체 명명 규칙에 "**group**"이라는 단어가 있습니다.

Show System Objects(시스템 개체 표시**)**를 선택했으므로 결과에 시스템 개체와 사용자 정의 개체가 모두 포함됩니다.

시스템 정의 개체 표시 필터

일부 디바이스는 공통 서비스에 대해 사전 정의된 개체가 함께 제공됩니다. 이러한 시스템 개체는 이미 생성되어 규칙 및 정책에서 사용할 수 있으므로 편리합니다. 개체 테이블에는 여러 시스템 개체가 있을 수 있습니다. 시스템 개체는 편집하거나 삭제할 수 없습니다.

Show System-Defined Objects(시스템 정의 개체 표시**)**는 기본적으로 꺼져 있습니다. 개체 테이블에 시스템 개체를 표시하려면 필터 표시줄에서 **Show System-Defined Objects(**시스템 정의 개체 표시**)**를 선택합니다. 개체 테이블에서 시스템 개체를 숨기려면 필터 표시줄에서 Show System Objects(시스템 개체 표시)를 선택하지 않은 상태로 둡니다.

시스템 개체를 숨기면 검색 및 필터링 결과에 포함되지 않습니다. 시스템 개체를 표시하면 개체 검색 및 필터링 결과에 포함됩니다.

개체 필터 구성

원하는 만큼 기준을 필터링할 수 있습니다. 더 많은 범주를 필터링할수록 예상되는 결과는 줄어듭니다.

Procedure

단계 **1** 왼쪽 창에서 **Objects(**개체**)**를 클릭합니다.

단계 **2** 페이지 상단의 필터 아이콘 을 클릭하여 필터 패널을 엽니다. 선택한 필터를 선택 취소하여 실수로 필터링된 개체가 없는지 확인합니다. 또한 검색 필드를 살펴보고 검색 필드에 입력되었을 수 있는 텍스트를 삭제합니다.

단계 **3** 특정 디바이스에 있는 것으로 결과를 제한하려면 다음을 수행합니다.

a. **Filter By Device(**디바이스별 필터링**)**를 클릭합니다.

b. 모든 디바이스를 검색하거나 디바이스 탭을 클릭하여 특정 종류의 디바이스만 검색합니다.

c. 필터 기준에 포함할 디바이스를 선택합니다.

d. **OK(**확인**)**를 클릭합니다.

단계 **4** 검색 결과에 시스템 개체를 포함하려면 **Show System Objects(**시스템 개체 표시**)**를 선택합니다. 검색 결과에서 시스템 개체를 제외하려면 **Show System Objects(**시스템 개체 표시**)**의 선택을 취소합니다.

단계 **5** 필터링할 개체 **Issues(**문제**)**를 선택합니다. 두 개 이상의 문제를 선택하면 선택한 범주의 개체가 필터 결과에 포함됩니다.

단계 **6** 문제가 있었지만 관리자가 무시한 개체를 확인하려면 **Ignored(**무시됨**)** 문제를 선택합니다.

단계 **7** 두 개 이상의 디바이스 간에 공유되는 개체를 필터링하는 경우 **Shared Objects(**공유 개체**)**에서 필수 필터를 선택합니다.

- **Default Values(**기본값**)**: 기본값만 있는 개체를 필터링합니다.
- **Override Values(**값 재정의**)**: 재정의된 값이 있는 개체를 필터링합니다.
- **Additional Values(**추가 값**)**: 추가 값이 있는 개체를 필터링합니다.

단계 **8** 규칙 또는 정책의 일부가 아닌 개체를 필터링하는 경우 **Unassociated(**연결되지 않음**)**를 선택합니다.

단계 **9** 필터링할 개체 유형을 선택합니다.

단계 **10** Objects(개체) 검색 필드에 개체 이름, IP 주소 또는 포트 번호를 추가하여 필터링된 결과 중에서 검색 기준으로 개체를 찾을 수도 있습니다.

필터 기준에서 디바이스를 제외해야 하는 경우

필터링 기준에 디바이스를 추가하면 결과에 디바이스의 개체가 표시되지만 해당 개체와 다른 디바이스의 관계는 표시되지 않습니다. 예를 들어 **ObjectA**가 ASA1과 ASA2 간에 공유된다고 가정합니다. ASA1에서 공유 개체를 찾기 위해 개체를 필터링하는 경우 **ObjectA**를 찾을 수 있지만 **Relationships(**관계**)** 창에는 해당 개체가 ASA1에 있다는 것만 표시됩니다.

개체와 관련된 모든 디바이스를 보려면 검색 기준에 디바이스를 지정하지 마십시오. 다른 기준으로 필터링하고 원하는 경우 검색 기준을 추가하십시오. Security Cloud Control가 식별하는 개체를 선택한 다음 관계 창을 살펴봅니다. 개체와 관련된 모든 디바이스 및 정책이 표시됩니다.

개체 무시 취소

사용되지 않거나 중복되거나 일관성이 없는 개체를 해결하는 한 가지 방법은 해당 개체를 무시하는 것입니다. 개체가 사용되지 않거나 중복되거나 일관성이 없더라도 해당 상태에 대한 타당한 이유가 있다고 판단하고 개체 문제를 해결되지 않은 상태로 두도록 선택할 수 있습니다. 나중에 무시된 개체를 해결해야 할 수도 있습니다. Security Cloud Control는 개체 문제를 검색할 때 무시된 개체를 표시하지 않으므로 무시된 개체에 대한 개체 목록을 필터링한 다음 결과에 따라 조치를 취해야 합니다.

Procedure

단계 **1** 왼쪽 창에서 **Objects(**개체**)**를 클릭하고 옵션을 선택합니다.
단계 **2** 무시된 개체를 필터링하고 검색합니다.
단계 **3** **Object(**개체**)** 테이블에서 무시를 취소할 개체를 선택합니다. 한 번에 하나의 개체를 무시 취소할 수 있습니다.
단계 **4** 세부 정보 창에서 **Unignore(**무시**)**를 클릭합니다.
단계 **5** 요청을 확인합니다. 이제 문제별로 개체를 필터링하면 이전에 무시되었던 개체를 찾아야 합니다.

개체 삭제

단일 개체 또는 여러 개체를 삭제할 수 있습니다.

단일 개체 삭제

Caution 클라우드 제공 Firewall Management Center가 테넌트에 구축된 경우:

ASA, FDM 및 FTD 네트워크 개체 및 그룹에 대한 변경 사항은 해당 클라우드 제공 Firewall Management Center 네트워크 개체 또는 그룹에 반영됩니다. 또한 **Discover & Manage Network Objects(**네트워크 개체 검색 및 관리**)**가 활성화된 각 온프레미스 방화벽 Management Center에 대한 **Devices with Pending Changes(**보류 중인 변경 사항이 있는 디바이스**)** 페이지에 항목이 생성됩니다. 여기에서 변경 사항을 선택하고 개체가 있는 온프레미스 방화벽 Management Center에 구축할 수 있습니다.

한 페이지에서 네트워크 개체 또는 그룹을 삭제하면 두 페이지 모두에서 개체 또는 그룹이 삭제됩니다.

Procedure

단계 **1** 왼쪽 창에서 **Objects(**개체**)**를 클릭합니다.
단계 **2** 개체 필터와 검색 필드를 사용하여 삭제하려는 개체를 찾아 선택합니다.
단계 **3** **Relationships(**관계**)** 창을 검토합니다. 개체가 정책 또는 개체 그룹에서 사용되는 경우 해당 정책 또는 그룹에서 개체를 제거할 때까지 개체를 삭제할 수 없습니다.
단계 **4** 작업 창에서 **Remove(**제거**)** 아이콘 를 클릭합니다.
단계 **5** **OK(**확인**)**을 클릭하여 개체 삭제를 확인합니다.
단계 **6** 변경 사항을 검토하고 구축하거나 기다렸다가 여러 변경 사항을 한 번에 구축합니다.

사용되지 않는 개체 그룹 삭제

디바이스를 온보딩하고 개체 문제를 해결하기 시작하면 사용하지 않는 개체를 많이 찾습니다. 한 번에 최대 50개의 사용하지 않는 개체를 삭제할 수 있습니다.

프로시저

단계 **1** **Issues(**문제**)** 필터를 사용하여 미사용 개체를 찾습니다. 디바이스 필터를 사용하여 디바이스 없음을 선택하여 디바이스와 연결되지 않은 개체를 찾을 수도 있습니다. 개체 목록을 필터링하면 개체 확인란이 나타납니다.

단계 **2** 개체 테이블 머리글에서 **Select all(**모두 선택**)** 확인란을 선택하여 개체 테이블에 나타나는 필터에 의해 발견된 모든 개체를 선택합니다. 또는 삭제할 개별 개체에 대한 개별 확인란을 선택합니다.

단계 **3** 작업 창에서 **Remove(**제거**)** 아이콘 를 클릭합니다.

단계 **4** 지금 변경 사항을 검토하고 구축하거나 기다렸다가 여러 변경 사항을 한 번에 구축합니다.

네트워크 개체

네트워크 개체는 호스트 이름, 네트워크 IP 주소, IP 주소의 범위, FQDN(인증된 도메인 이름) 또는 CIDR 표기법으로 표현된 서브 네트워크를 포함할 수 있습니다. 네트워크 그룹은 그룹에 추가하는 네트워크 개체 및 기타 개별 주소 또는 서브 네트워크의 모음입니다. 네트워크 개체 및 네트워크 그룹은 액세스 규칙, 네트워크 정책 및 NAT 규칙에서 사용됩니다.

동적 개체를 공유할 때 Cisco Meraki 및 Multicloud Defense 등 모든 플랫폼이 네트워크 개체를 지원하는 것은 아니며, Security Cloud Control는 원본 플랫폼 또는 디바이스에서 적절한 정보를 Security Cloud Control이 사용할 수 있는 사용 가능한 정보 집합으로 자동으로 변환합니다.

제품 간 네트워크 개체 재사용

Security Cloud Control 테넌트가 하나 있고 클라우드 제공 Firewall Management Center 및 하나 이상의 온프레미스 방화벽 Management Center가 테넌트에 온보딩된 경우:

- Secure Firewall Threat Defense, FDM 관리 Firewall Threat Defense, ASA 또는 Meraki 네트워크 개체 또는 그룹을 생성하면 클라우드 제공 Firewall Management Center를 구성할 때 사용되는 **Objects(**개체**)** 페이지의 개체 목록에도 개체의 복사본이 추가되며, 그 반대의 경우도 마찬가지입니다.
- Secure Firewall Threat Defense, FDM 관리 Firewall Threat Defense 또는 ASA 네트워크 개체나 그룹을 생성하면 **Devices with Pending Changes(**보류 중인 변경 사항이 있는 디바이스**)** 페이지에 **Discover & Manage Network Objects(**네트워크 개체 검색 및 관리**)**가 활성화된 각 온프레미스 방화벽 Management Center에 대해 항목이 생성됩니다. 이 목록에서 개체를 사용하려는 온프레미스 방화벽 Management Center에 개체를 선택하여 구축하고 원하지 않는 개체를 폐기할 수 있습니다. ,**Administration(**관리**)** > **Firewall Management Center** 로 이동하고 온프레미스 방화벽 Management Center를 선택한 후 **Objects(**개체**)**를 클릭하여 온프레미스 방화벽 Management Center 사용자 인터페이스에서 개체를 확인하고 정책에 할당합니다.

한 페이지에서 네트워크 개체 또는 그룹에 대한 변경 사항은 두 페이지의 개체 또는 그룹 인스턴스에 적용됩니다. 한 페이지에서 개체를 삭제하면 다른 페이지에서도 개체의 해당 복사본이 삭제됩니다.

예외:

- 클라우드 제공 Firewall Management Center에 대해 동일한 이름의 네트워크 개체가 이미 있는 경우, 새로운 Secure Firewall Threat Defense, FDM 관리 Firewall Threat Defense, ASA 또는 Meraki 네트워크 개체는 Security Cloud Control의 **Objects(**개체**)** 페이지에서 복제되지 않습니다.
- 온프레미스 Secure Firewall Management Center에서 관리하는 온보딩된 Firewall Threat Defense 디바이스의 네트워크 개체 및 그룹은 복제되지 않으며, 클라우드 제공 Firewall Management Center에서 사용할 수 없습니다.

  클라우드 제공 Firewall Management Center로 마이그레이션된 온프레미스 Secure Firewall Management Center 인스턴스의 경우, 네트워크 개체 및 그룹이 FTD 디바이스에 구축된 정책에서 사용되었다면 네트워크 개체 및 그룹이 Security Cloud Control 개체 페이지에 복제됩니다.
- Security Cloud Control와 클라우드 제공 Firewall Management Center 간에 네트워크 개체 공유는 새로운 테넌트에서 자동으로 활성화되지만 기존 테넌트에 대해서는 요청해야 합니다. 네트워크 개체를 클라우드 제공 Firewall Management Center와 공유하지 않는 경우 TAC에 문의하여 테넌트에서 기능을 활성화하십시오.
- Security Cloud Control와 온프레미스 방화벽 Management Center간의 네트워크 개체 공유는 Security Cloud Control에 온보딩된 새 온프레미스 방화벽 Management Center에 대해 Security Cloud Control에서 자동으로 활성화되지 않습니다. 네트워크 개체가 온프레미스 방화벽 Management Center와 공유되지 않는 경우 **Settings(**설정**)**에서 온프레미스 방화벽 Management Center에 대해 **Discover & Manage Network Objects(**네트워크 개체 검색 및 관리**)** 토글 버튼이 활성화되어 있는지 확인하거나 TAC에 문의하여 테넌트에서 기능을 활성화하십시오.

네트워크 개체 보기

Security Cloud Control를 사용하여 생성한 네트워크 개체와 온보딩된 디바이스 구성에서 Security Cloud Control가 인식것이 Objects(개체) 페이지에 표시됩니다. 개체 유형으로 레이블이 지정됩니다. 이렇게 하면 개체 유형으로 필터링하여 원하는 개체를 빠르게 찾을 수 있습니다.

Objects(개체) 페이지에서 네트워크 개체를 선택하면 Details(세부 정보) 창에 개체의 값이 표시됩니다. Relationships(관계) 창에는 개체가 정책에서 사용되는지 여부와 개체가 저장된 디바이스가 표시됩니다.

네트워크 그룹을 클릭하면 해당 그룹의 콘텐츠가 표시됩니다. 네트워크 그룹은 네트워크 개체에 의해 제공되는 모든 값의 복합물입니다.

ASA 네트워크 개체 및 네트워크 그룹 생성 또는 편집

ASA 네트워크 개체는 CIDR 표기법으로 표시된 호스트 이름, IP 주소 또는 서브넷 주소를 포함할 수 있습니다. 네트워크 그룹은 액세스 규칙, 네트워크 정책 및 NAT 규칙에 사용되는 네트워크 개체, 네트워크 그룹 및 IP 주소의 복합 그룹입니다. Security Cloud Control을 사용하여 네트워크 개체 및 네트워크 그룹을 생성, 읽기, 업데이트 및 삭제할 수 있습니다.

Table 3: ASA 네트워크 개체 및 그룹의 허용 값

디바이스 유형	**IPv4 / IPv6**	단일 주소	주소 범위	**PQDN(Partially Qualified Domain Name)**	**CIDR** 표기법의 서브넷
ASA	IPv4 / IPv6	예	예	예	예

Note 클라우드 제공 Firewall Management Center가 테넌트에 구축된 경우:

Objects(개체**)** 페이지에서 FTD, FDM 또는 ASA 네트워크 개체 또는 그룹을 생성하면 개체의 복사본이 클라우드 제공 Firewall Management Center에 자동으로 추가되며 그 반대의 경우도 마찬가지입니다. 또한 **Discover & Manage Network Objects(**네트워크 개체 검색 및 관리**)**가 활성화된 각 온프레미스 방화벽 Management Center에 대한 **Devices with Pending Changes(**보류 중인 변경 사항이 있는 디바이스**)** 페이지에 항목이 생성됩니다. 여기에서 개체를 선택하고 개체가 있는 온프레미스 방화벽 Management Center에 구축할 수 있습니다.

Caution 클라우드 제공 Firewall Management Center가 테넌트에 구축된 경우:

ASA, FDM 및 FTD 네트워크 개체 및 그룹에 대한 변경 사항은 해당 클라우드 제공 Firewall Management Center 네트워크 개체 또는 그룹에 반영됩니다. 또한 **Discover & Manage Network Objects(**네트워크 개체 검색 및 관리**)**가 활성화된 각 온프레미스 방화벽 Management Center에 대한 **Devices with Pending Changes(**보류 중인 변경 사항이 있는 디바이스**)** 페이지에 항목이 생성됩니다. 여기에서 변경 사항을 선택하고 개체가 있는 온프레미스 방화벽 Management Center에 구축할 수 있습니다.

한 페이지에서 네트워크 개체 또는 그룹을 삭제하면 두 페이지 모두에서 개체 또는 그룹이 삭제됩니다.

ASA 네트워크 개체 생성

네트워크 개체는 호스트 이름, 네트워크 IP 주소, IP 주소의 범위, FQDN(인증된 도메인 이름) 또는 CIDR 표기법으로 표현된 서브 네트워크를 포함할 수 있습니다. 네트워크 개체는 액세스 규칙, 네트워크 정책 및 NAT 규칙에서 사용됩니다. Security Cloud Control을 사용하여 네트워크 개체 및 네트워크 그룹을 생성, 업데이트 및 삭제할 수 있습니다.

Note 클라우드 제공 Firewall Management Center가 테넌트에 구축된 경우:

Objects(개체**)** 페이지에서 FTD, FDM 또는 ASA 네트워크 개체 또는 그룹을 생성하면 개체의 복사본이 클라우드 제공 Firewall Management Center에 자동으로 추가되며 그 반대의 경우도 마찬가지입니다. 또한 **Discover & Manage Network Objects(**네트워크 개체 검색 및 관리**)**가 활성화된 각 온프레미스 방화벽 Management Center에 대한 **Devices with Pending Changes(**보류 중인 변경 사항이 있는 디바이스**)** 페이지에 항목이 생성됩니다. 여기에서 개체를 선택하고 개체가 있는 온프레미스 방화벽 Management Center에 구축할 수 있습니다.

Procedure

단계 **1** 왼쪽 창에서 개체를 클릭합니다.

단계 **2** 파란색 플러스 버튼  을 클릭하여 개체를 생성합니다.

단계 **3** **ASA** > **Network(ASA** 네트워크**)**를 클릭합니다.

단계 **4** 개체 이름을 입력합니다.

단계 **5** **Create a network object(**네트워크 개체 생성**)**를 선택합니다.

단계 **6** (선택 사항) 개체 설명을 입력합니다.

단계 **7** **Value(**값**)** 섹션에서 다음 방법 중 하나로 IP 주소 정보를 추가합니다.

- **eq**를 선택한 다음 단일 IP 주소, CIDR 표기법을 사용한 서브넷 주소 또는 PQDN(Partially Qualified Domain Name)을 입력합니다.
- 범위를 선택한 다음 IP 주소의 범위를 입력합니다. 시작 주소와 끝 주소를 공백으로 구분하여 범위를 입력합니다. 예: 10.1.1.1 10.1.1.255 또는 2001:DB8:1::1 2001:DB8:1::3

단계 **8** **Add(**추가**)**를 클릭합니다.

Important
새로 생성된 네트워크 개체는 규칙 또는 정책의 일부가 아니므로 ASA 디바이스와 연결되지 않습니다. 이러한 개체를 보려면 개체 필터에서 **Unassociated(**연결되지 않음**)** 개체 범주를 선택합니다.

자세한 내용은 개체 필터를 참조하십시오. 디바이스의 규칙 또는 정책에서 연결되지 않은 개체를 사용하면 이러한 개체는 해당 디바이스와 연결됩니다.

ASA 네트워크 그룹 생성

네트워크 그룹은 IP 주소 값, 네트워크 개체 및 네트워크 그룹을 포함할 수 있습니다. 새 네트워크 그룹을 만들 때 이름, IP 주소, IP 주소 범위 또는 FQDN으로 기존 개체를 검색하고 네트워크 그룹에 추가할 수 있습니다. 개체가 없는 경우 동일한 인터페이스에서 해당 개체를 즉시 생성하고 네트워크 그룹에 추가할 수 있습니다. 네트워크 그룹은 IPv4 및 IPv6 주소를 모두 포함할 수 있습니다.

Note 클라우드 제공 Firewall Management Center가 테넌트에 구축된 경우:

Objects(개체**)** 페이지에서 FTD, FDM 또는 ASA 네트워크 개체 또는 그룹을 생성하면 개체의 복사본이 클라우드 제공 Firewall Management Center에 자동으로 추가되며 그 반대의 경우도 마찬가지입니다. 또한 **Discover & Manage Network Objects(**네트워크 개체 검색 및 관리**)**가 활성화된 각 온프레미스 방화벽 Management Center에 대한 **Devices with Pending Changes(**보류 중인 변경 사항이 있는 디바이스**)** 페이지에 항목이 생성됩니다. 여기에서 개체를 선택하고 개체가 있는 온프레미스 방화벽 Management Center에 구축할 수 있습니다.

Procedure

단계 **1** 왼쪽 창에서 개체를 클릭합니다.

단계 **2** 파란색 플러스 버튼  을 클릭하여 개체를 생성합니다.

단계 **3** **ASA** > **Network(ASA** 네트워크**)**를 클릭합니다.

단계 **4** 개체 이름을 입력합니다.

단계 **5** **Create a network group(**네트워크 그룹 생성**)**을 선택합니다.

단계 **6** (선택 사항) 개체 설명을 입력합니다.

단계 **7** **Values(**값**)** 필드에 값 또는 개체 이름을 입력합니다. 입력을 시작하면 Security Cloud Control에서 항목과 일치하는 개체 이름 또는 값을 제공합니다.

단계 **8** 표시된 기존 개체 중 하나를 선택하거나 입력한 이름 또는 값을 기반으로 새 개체를 생성할 수 있습니다.

단계 **9** Security Cloud Control가 일치하는 항목을 찾은 경우 기존 개체를 선택하려면 **Add(**추가**)**를 클릭하여 네트워크 개체 또는 네트워크 그룹을 새 네트워크 그룹에 추가합니다.

단계 **10** 존재하지 않는 값 또는 개체를 입력한 경우 다음 중 하나를 수행할 수 있습니다.

- 해당 이름으로 새 개체를 생성하려면 **Add as New Object With This Name(**이 이름의 새 개체로 추가**)**을 클릭합니다. 값을 입력하고 확인 표시를 클릭하여 저장합니다.
- 새 개체를 생성하려면 **Add as New Object(**새 개체로 추가**)**를 클릭합니다. 개체 이름과 값이 동일합니다. 이름을 입력하고 확인 표시를 클릭하여 저장합니다.
- 개체를 사용하지 않고 인라인 값을 만들려면 **Add Value(**값 추가**)**를 클릭합니다. 값을 입력하고 확인 표시를 클릭하여 저장합니다.

값이 이미 있는 경우에도 새 개체를 생성할 수 있습니다. 이러한 개체를 변경하고 저장할 수 있습니다.

Note
편집 아이콘을 클릭하여 세부 정보를 편집할 수 있습니다. 삭제 버튼을 클릭해도 개체 자체는 삭제되지 않습니다. 대신 네트워크 그룹에서 제거됩니다.

단계 **11** 필요한 개체를 추가한 후 **Add(**추가**)**를 클릭하여 새 네트워크 그룹을 생성합니다.

단계 **12** 모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축.

ASA 네트워크 개체 편집

Caution 클라우드 제공 Firewall Management Center가 테넌트에 구축된 경우:

ASA, FDM 및 FTD 네트워크 개체 및 그룹에 대한 변경 사항은 해당 클라우드 제공 Firewall Management Center 네트워크 개체 또는 그룹에 반영됩니다. 또한 **Discover & Manage Network Objects(**네트워크 개체 검색 및 관리**)**가 활성화된 각 온프레미스 방화벽 Management Center에 대한 **Devices with Pending Changes(**보류 중인 변경 사항이 있는 디바이스**)** 페이지에 항목이 생성됩니다. 여기에서 변경 사항을 선택하고 개체가 있는 온프레미스 방화벽 Management Center에 구축할 수 있습니다.

한 페이지에서 네트워크 개체 또는 그룹을 삭제하면 두 페이지 모두에서 개체 또는 그룹이 삭제됩니다.

Procedure

단계 **1** 왼쪽 창에서 개체를 클릭합니다.

단계 **2** 개체 필터 및 검색 필드를 사용하여 편집할 개체를 찾습니다.

단계 **3** 네트워크 개체를 선택하고 **Actions(**작업**)** 창에서 편집 아이콘 을 클릭합니다.

단계 **4** 위의 절차에서 만든 것과 같은 방식으로 대화 상자에서 값을 수정합니다.

Note
네트워크 그룹에서 개체를 제거하려면 옆에 있는 삭제 아이콘을 클릭합니다.

단계 **5** **Save(**저장**)**를 클릭합니다. Security Cloud Control는 변경의 영향을 받는 디바이스를 표시합니다.

단계 **6** **Confirm(**확인**)**을 클릭하여 개체 및 해당 개체의 영향을 받는 모든 디바이스에 대한 변경을 완료합니다.

ASA 네트워크 그룹 편집

Caution 클라우드 제공 Firewall Management Center가 테넌트에 구축된 경우:

ASA, FDM 및 FTD 네트워크 개체 및 그룹에 대한 변경 사항은 해당 클라우드 제공 Firewall Management Center 네트워크 개체 또는 그룹에 반영됩니다. 또한 **Discover & Manage Network Objects(**네트워크 개체 검색 및 관리**)**가 활성화된 각 온프레미스 방화벽 Management Center에 대한 **Devices with Pending Changes(**보류 중인 변경 사항이 있는 디바이스**)** 페이지에 항목이 생성됩니다. 여기에서 변경 사항을 선택하고 개체가 있는 온프레미스 방화벽 Management Center에 구축할 수 있습니다.

한 페이지에서 네트워크 개체 또는 그룹을 삭제하면 두 페이지 모두에서 개체 또는 그룹이 삭제됩니다.

Procedure

단계 **1** 왼쪽 창에서 개체를 클릭합니다.

단계 **2** 개체 필터 및 검색 필드를 사용하여 편집하려는 네트워크 그룹을 찾습니다.

단계 **3** SGT 그룹을 선택하고 **Actions(**작업**)** 창에서 편집 아이콘 를 클릭합니다.

단계 **4** 이 네트워크 그룹에 새 네트워크 개체 또는 네트워크 그룹을 추가하려면 다음 단계를 수행합니다.

a. 개체 이름 또는 네트워크 그룹 옆에 나타나는 편집 아이콘 을 클릭하여 수정합니다.

b. 확인 표시를 클릭하여 변경 사항을 저장합니다.

Note
네트워크 그룹에서 값을 제거하려면 삭제 아이콘을 클릭합니다.

단계 **5** 이 네트워크 그룹에 새 네트워크 개체 또는 네트워크 그룹을 추가하려면 다음 단계를 수행합니다.

a. **Values(**값**)** 필드에 새 값이나 기존 네트워크 개체의 이름을 입력합니다. 입력을 시작하면 Security Cloud Control에서 항목과 일치하는 개체 이름 또는 값을 제공합니다. 표시된 기존 개체 중 하나를 선택하거나 입력한 이름 또는 값을 기반으로 새 개체를 생성할 수 있습니다.

b. Security Cloud Control가 일치하는 항목을 찾은 경우 기존 개체를 선택하려면 **Add(**추가**)**를 클릭하여 네트워크 개체 또는 네트워크 그룹을 새 네트워크 그룹에 추가합니다.

c. 존재하지 않는 값 또는 개체를 입력한 경우 다음 중 하나를 수행할 수 있습니다.

- 해당 이름으로 새 개체를 생성하려면 **Add as New Object With This Name(**이 이름의 새 개체로 추가**)**을 클릭합니다. 값을 입력하고 확인 표시를 클릭하여 저장합니다.
- 새 개체를 생성하려면 **Add as New Object(**새 개체로 추가**)**를 클릭합니다. 개체 이름과 값이 동일합니다. 이름을 입력하고 확인 표시를 클릭하여 저장합니다.
- 개체를 사용하지 않고 인라인 값을 만들려면 **Add Value(**값 추가**)**를 클릭합니다. 값을 입력하고 확인 표시를 클릭하여 저장합니다.

값이 이미 있는 경우에도 새 개체를 생성할 수 있습니다. 이러한 개체를 변경하고 저장할 수 있습니다.

단계 **6** **Save(**저장**)**를 클릭합니다. Security Cloud Control는 변경의 영향을 받는 정책을 표시합니다.

단계 **7** **Confirm(**확인**)**을 클릭하여 개체 및 해당 개체의 영향을 받는 모든 디바이스에 대한 변경을 완료합니다.

단계 **8** 모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축.

Security Cloud Control의 공유 네트워크 그룹에 추가 값 추가

공유 네트워크 그룹에 연결된 모든 디바이스에 있는 값을 "기본값"이라고 합니다. Security Cloud Control은 공유 네트워크 그룹에 "추가 값"을 추가하고 해당 공유 네트워크 그룹과 연결된 일부 디바

이스에 해당 값을 할당할 수 있습니다. Security Cloud Control는 변경 사항을 디바이스에 구축할 때 콘텐츠를 확인하고 공유 네트워크 그룹과 연결된 모든 디바이스에 "기본값"을 푸시하고 지정된 디바이스에만 "추가 값"을 푸시합니다.

모든 사이트에서 액세스할 수 있어야 하는 본사에 4개의 AD 기본 서버가 있는 시나리오를 예로 들어 보겠습니다. 따라서 모든 사이트에서 사용할 "Active-Directory"라는 개체 그룹을 생성했습니다. 이제 지사 중 하나에 두 개의 AD 서버를 추가하려고 합니다. 개체 그룹 "Active-Directory"에서 해당 지사에 특정한 추가 값으로 세부 정보를 추가하여 이 작업을 수행할 수 있습니다. 이 두 서버는 "Active-Directory" 개체가 일관성이 있는지 또는 공유되는지를 확인하는 데 참여하지 않습니다. 따라서 모든 사이트에서 4개의 AD 기본 서버에 액세스할 수 있지만 지사(2개의 추가 서버 포함)는 2개의 AD 서버와 4개의 AD 기본 서버에 액세스할 수 있습니다.

Note 일치하지 않는 공유 네트워크 그룹이 있는 경우 추가 값을 사용하여 단일 공유 네트워크 그룹으로 결합할 수 있습니다. 자세한 내용은 일관되지 않은 개체 문제 해결을 참조하십시오.

Caution 클라우드 제공 Firewall Management Center가 테넌트에 구축된 경우:

ASA, FDM 및 FTD 네트워크 개체 및 그룹에 대한 변경 사항은 해당 클라우드 제공 Firewall Management Center 네트워크 개체 또는 그룹에 반영됩니다. 또한 **Discover & Manage Network Objects(**네트워크 개체 검색 및 관리**)**가 활성화된 각 온프레미스 방화벽 Management Center에 대한 **Devices with Pending Changes(**보류 중인 변경 사항이 있는 디바이스**)** 페이지에 항목이 생성됩니다. 여기에서 변경 사항을 선택하고 개체가 있는 온프레미스 방화벽 Management Center에 구축할 수 있습니다.

한 페이지에서 네트워크 개체 또는 그룹을 삭제하면 두 페이지 모두에서 개체 또는 그룹이 삭제됩니다.

Procedure

단계 **1** 왼쪽 창에서 개체를 클릭합니다.

단계 **2** 개체 필터 및 검색 필드를 사용하여 편집할 공유 네트워크 그룹을 찾습니다.

단계 **3** **Actions(**작업**)** 창에서 편집 아이콘 을 클릭합니다.

- **Devices(**디바이스**)** 필드에는 공유 네트워크 그룹이 있는 디바이스가 표시됩니다.
- **Usage(**사용**)** 필드에는 공유 네트워크 그룹과 연결된 규칙 집합이 표시됩니다.
- **Default Values(**기본값**)** 필드는 생성 중에 제공된 공유 네트워크 그룹과 연결된 기본 네트워크 개체 및 해당 값을 지정합니다. 이 필드 옆에서 이 기본값이 포함된 디바이스의 수를 볼 수 있으며, 클릭하여 해당 이름 및 디바이스 유형을 볼 수 있습니다. 이 값과 연결된 규칙 집합도 확인할 수 있습니다.

단계 **4** 추가 값 필드에 값 또는 이름을 입력합니다. 입력을 시작하면 Security Cloud Control에서 항목과 일치하는 개체 이름 또는 값을 제공합니다.

단계 **5** 표시된 기존 개체 중 하나를 선택하거나 입력한 이름 또는 값을 기반으로 새 개체를 생성할 수 있습니다.

단계 **6** Security Cloud Control가 일치하는 항목을 찾은 경우 기존 개체를 선택하려면 **Add(**추가**)**를 클릭하여 네트워크 개체 또는 네트워크 그룹을 새 네트워크 그룹에 추가합니다.

단계 **7** 존재하지 않는 값 또는 개체를 입력한 경우 다음 중 하나를 수행할 수 있습니다.

- 해당 이름으로 새 개체를 생성하려면 **Add as New Object With This Name(**이 이름의 새 개체로 추가**)**을 클릭합니다. 값을 입력하고 확인 표시를 클릭하여 저장합니다.
- 새 개체를 생성하려면 **Add as New Object(**새 개체로 추가**)**를 클릭합니다. 개체 이름과 값이 동일합니다. 이름을 입력하고 확인 표시를 클릭하여 저장합니다.
- 개체를 사용하지 않고 인라인 값을 만들려면 **Add Value(**값 추가**)**를 클릭합니다. 값을 입력하고 확인 표시를 클릭하여 저장합니다.

값이 이미 있는 경우에도 새 개체를 생성할 수 있습니다. 이러한 개체를 변경하고 저장할 수 있습니다.

단계 **8** **Devices(**디바이스**)** 열에서 새로 추가된 개체와 연결된 셀을 클릭하고 **Add Devices(**디바이스 추가**)**를 클릭합니다.

단계 **9** 원하는 디바이스를 선택하고 **OK(**확인**)**를 클릭합니다.

단계 **10** **Save(**저장**)**를 클릭합니다. Security Cloud Control는 변경의 영향을 받는 디바이스를 표시합니다.

단계 **11** **Confirm(**확인**)**을 클릭하여 개체 및 해당 개체의 영향을 받는 모든 디바이스에 대한 변경을 완료합니다.

단계 **12** 모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축.

Security Cloud Control에서 공유 네트워크 그룹의 추가 값 편집

Caution 클라우드 제공 Firewall Management Center가 테넌트에 구축된 경우:

ASA, FDM 및 FTD 네트워크 개체 및 그룹에 대한 변경 사항은 해당 클라우드 제공 Firewall Management Center 네트워크 개체 또는 그룹에 반영됩니다. 또한 **Discover & Manage Network Objects(**네트워크 개체 검색 및 관리**)**가 활성화된 각 온프레미스 방화벽 Management Center에 대한 **Devices with Pending Changes(**보류 중인 변경 사항이 있는 디바이스**)** 페이지에 항목이 생성됩니다. 여기에서 변경 사항을 선택하고 개체가 있는 온프레미스 방화벽 Management Center에 구축할 수 있습니다.

한 페이지에서 네트워크 개체 또는 그룹을 삭제하면 두 페이지 모두에서 개체 또는 그룹이 삭제됩니다.

Procedure

단계 **1** 왼쪽 창에서 개체를 클릭합니다.

단계 **2** 개체 필터 및 검색 필드를 사용하여 편집하려는 재정의가 있는 개체를 찾습니다.

단계 **3** **Actions(**작업**)** 창에서 편집 아이콘 을 클릭합니다.

단계 **4** 재정의 값을 수정합니다.

- 값을 편집하려면 편집 아이콘을 클릭합니다.
- **Devices(**디바이스**)** 열의 셀을 클릭하여 새 디바이스를 할당합니다. 이미 할당된 디바이스를 선택하고 **Remove Overrides(**재정의 제거**)**를 클릭하여 해당 디바이스에서 재정의를 제거할 수 있습니다.
- **Default Values(**기본값**)**의 화살표를 클릭하여 푸시하고 공유 네트워크 그룹의 추가 값으로 설정합니다. 공유 네트워크 그룹과 연결된 모든 디바이스가 자동으로 할당됩니다.
- **Override Values(**값 재정의**)**에서 화살표를 클릭하여 공유 네트워크 그룹의 기본 개체로 푸시하고 설정합니다.
- 네트워크 그룹에서 개체를 제거하려면 옆에 있는 삭제 아이콘을 클릭합니다.

단계 **5** **Save(**저장**)**를 클릭합니다. Security Cloud Control는 변경의 영향을 받는 디바이스를 표시합니다.

단계 **6** **Confirm(**확인**)**을 클릭하여 개체 및 해당 개체의 영향을 받는 모든 디바이스에 대한 변경을 완료합니다.

단계 **7** 모든 디바이스에 대한 구성 변경 사항 미리보기 및 구축.

Security Cloud Control에서 네트워크 개체 및 그룹 삭제

클라우드 제공 Firewall Management Center가 테넌트에 구축된 경우:

개체 페이지에서 네트워크 개체 또는 그룹을 삭제하면 클라우드 제공 Firewall Management Center의 개체 페이지에서 복제된 네트워크 개체 또는 그룹이 삭제되며, 그 반대의 경우도 마찬가지입니다.

Firepower 네트워크 개체 또는 네트워크 그룹 생성 또는 편집

Firepower 네트워크 개체는 CIDR 표기법으로 표시된 호스트 이름, IP 주소 또는 서브넷 주소를 포함할 수 있습니다. 네트워크 그룹은 액세스 규칙, 네트워크 정책 및 NAT 규칙에 사용되는 네트워크 개체 및 네트워크 그룹의 복합 그룹입니다. Security Cloud Control을 사용하여 네트워크 개체 및 네트워크 그룹을 생성, 읽기, 업데이트 및 삭제할 수 있습니다.

Firepower 네트워크 개체 및 그룹은 ASA, Firewall Threat Defense, FDM 관리 및 Meraki 디바이스에서 사용할 수 있습니다. 제품 간 네트워크 개체 재사용, on page 29을 참조하십시오.

Note 클라우드 제공 Firewall Management Center가 테넌트에 구축된 경우:

Objects(개체**)** 페이지에서 FTD, FDM 또는 ASA 네트워크 개체 또는 그룹을 생성하면 개체의 복사본이 클라우드 제공 Firewall Management Center에 자동으로 추가되며 그 반대의 경우도 마찬가지입니다. 또한 **Discover & Manage Network Objects(**네트워크 개체 검색 및 관리**)**가 활성화된 각 온프레미스 방화벽 Management Center에 대한 **Devices with Pending Changes(**보류 중인 변경 사항이 있는 디바이스**)** 페이지에 항목이 생성됩니다. 여기에서 개체를 선택하고 개체가 있는 온프레미스 방화벽 Management Center에 구축할 수 있습니다.

Caution 클라우드 제공 Firewall Management Center가 테넌트에 구축된 경우:

ASA, FDM 및 FTD 네트워크 개체 및 그룹에 대한 변경 사항은 해당 클라우드 제공 Firewall Management Center 네트워크 개체 또는 그룹에 반영됩니다. 또한 **Discover & Manage Network Objects(**네트워크 개체 검색 및 관리**)**가 활성화된 각 온프레미스 방화벽 Management Center에 대한 **Devices with Pending Changes(**보류 중인 변경 사항이 있는 디바이스**)** 페이지에 항목이 생성됩니다. 여기에서 변경 사항을 선택하고 개체가 있는 온프레미스 방화벽 Management Center에 구축할 수 있습니다.

한 페이지에서 네트워크 개체 또는 그룹을 삭제하면 두 페이지 모두에서 개체 또는 그룹이 삭제됩니다.

Table 4: 네트워크 개체에 추가할 수 있는 ***IP*** 주소

디바이스 유형	**IPv4 / IPv6**	단일 주소	주소 범위	**PQDN(Partially Qualified Domain Name)**	**CIDR** 표기법의 서브넷
Firepower	IPv4 / IPv6	예	예	예	예

관련 정보:

- Firepower 네트워크 개체 생성, on page 39
- Firepower 네트워크 개체 편집, on page 41
- 공유 네트워크 그룹에 값 추가, on page 44
- 공유 네트워크 그룹의 추가 값 편집, on page 46

Firepower 네트워크 개체 생성

Note 클라우드 제공 Firewall Management Center가 테넌트에 구축된 경우:

Objects(개체**)** 페이지에서 FTD, FDM 또는 ASA 네트워크 개체 또는 그룹을 생성하면 개체의 복사본이 클라우드 제공 Firewall Management Center에 자동으로 추가되며 그 반대의 경우도 마찬가지입니다. 또한 **Discover & Manage Network Objects(**네트워크 개체 검색 및 관리**)**가 활성화된 각 온프레미스 방화벽 Management Center에 대한 **Devices with Pending Changes(**보류 중인 변경 사항이 있는 디바이스**)** 페이지에 항목이 생성됩니다. 여기에서 개체를 선택하고 개체가 있는 온프레미스 방화벽 Management Center에 구축할 수 있습니다.

Procedure

단계 **1** 왼쪽 창에서 개체를 클릭합니다.

단계 **2** 파란색 플러스 버튼  을 클릭하여 개체를 생성합니다.

단계 **3** **FTD** > **Network(**네트워크**)**를 클릭합니다.

단계 **4** 개체 이름을 입력합니다.

단계 **5** **Create a network object(**네트워크 개체 생성**)**를 선택합니다.

단계 **6** **Value(**값**)** 섹션에서 다음을 수행합니다.

- **eq**를 선택하고 단일 IP 주소, CIDR 표기법으로 표시된 서브넷 주소 또는 PQDN(Partially Qualified Domain Name)을 입력합니다.
- 범위를 선택하고 IP 주소 범위를 입력합니다.

Note
호스트 비트 값을 설정하지 마십시오. 0이 아닌 호스트 비트 값을 입력하면 클라우드 제공 Firewall Management Center에서 호스트 비트가 설정되지 않은 IPv6 개체만 허용하므로 Security Cloud Control가 개체를 생성하는 동안 이 값을 설정 해제합니다.

단계 **7** **Add(**추가**)**를 클릭합니다.

주의: 새로 생성된 네트워크 개체는 규칙 또는 정책의 일부가 아니므로 FDM 관리 디바이스와 연결되지 않습니다. 이러한 개체를 보려면 개체 필터에서 **Unassociated(**연결되지 않음**)** 개체 범주를 선택합니다. 자세한 내용은 개체 필터를 참조하십시오. 디바이스의 규칙 또는 정책에서 연결되지 않은 개체를 사용하면 이러한 개체는 해당 디바이스와 연결됩니다.

Firepower 네트워크 그룹 생성

네트워크 그룹은 네트워크 개체와 네트워크 그룹을 포함할 수 있습니다. 새 네트워크 그룹을 만들 때 이름, IP 주소, IP 주소 범위 또는 FQDN으로 기존 개체를 검색하고 네트워크 그룹에 추가할 수 있습니다. 개체가 없는 경우 동일한 인터페이스에서 해당 개체를 즉시 생성하고 네트워크 그룹에 추가할 수 있습니다.

Note 클라우드 제공 Firewall Management Center가 테넌트에 구축된 경우:

Objects(개체**)** 페이지에서 FTD, FDM 또는 ASA 네트워크 개체 또는 그룹을 생성하면 개체의 복사본이 클라우드 제공 Firewall Management Center에 자동으로 추가되며 그 반대의 경우도 마찬가지입니다. 또한 **Discover & Manage Network Objects(**네트워크 개체 검색 및 관리**)**가 활성화된 각 온프레미스 방화벽 Management Center에 대한 **Devices with Pending Changes(**보류 중인 변경 사항이 있는 디바이스**)** 페이지에 항목이 생성됩니다. 여기에서 개체를 선택하고 개체가 있는 온프레미스 방화벽 Management Center에 구축할 수 있습니다.

Procedure

단계 **1** 왼쪽 창에서 개체를 클릭합니다.

단계 **2** 파란색 플러스 버튼  을 클릭하여 개체를 생성합니다.

단계 **3** **FTD** > **Network(**네트워크**)**를 클릭합니다.

단계 **4** 개체 이름을 입력합니다.

단계 **5** **Create a network group(**네트워크 그룹 생성**)**을 선택합니다.

단계 **6** 값 필드에 값이나 이름을 입력합니다. 입력을 시작하면 Security Cloud Control에서 항목과 일치하는 개체 이름 또는 값을 제공합니다.

단계 **7** 표시된 기존 개체 중 하나를 선택하거나 입력한 이름 또는 값을 기반으로 새 개체를 생성할 수 있습니다.

단계 **8** Security Cloud Control가 일치하는 항목을 찾은 경우 기존 개체를 선택하려면 **Add(**추가**)**를 클릭하여 네트워크 개체 또는 네트워크 그룹을 새 네트워크 그룹에 추가합니다.

단계 **9** 존재하지 않는 값 또는 개체를 입력한 경우 다음 중 하나를 수행할 수 있습니다.

- 해당 이름으로 새 개체를 생성하려면 **Add as New Object With This Name(**이 이름의 새 개체로 추가**)**을 클릭합니다. 값을 입력하고 확인 표시를 클릭하여 저장합니다.
- 새 개체를 생성하려면 **Add as New Object(**새 개체로 추가**)**를 클릭합니다. 개체 이름과 값이 동일합니다. 이름을 입력하고 확인 표시를 클릭하여 저장합니다.

값이 이미 있는 경우에도 새 개체를 생성할 수 있습니다. 이러한 개체를 변경하고 저장할 수 있습니다.

참고: 편집 아이콘을 클릭하여 세부 정보를 편집할 수 있습니다. 삭제 버튼을 클릭해도 개체 자체는 삭제되지 않습니다. 대신 네트워크 그룹에서 제거됩니다.

단계 **10** 필요한 개체를 추가한 후 **Save(**저장**)**을 클릭하여 새 네트워크 그룹을 생성합니다.

단계 **11** 모든 디바이스에 대한 구성 변경 사항을 미리보고 구축합니다.

Firepower 네트워크 개체 편집

Caution 클라우드 제공 Firewall Management Center가 테넌트에 구축된 경우:

ASA, FDM 및 FTD 네트워크 개체 및 그룹에 대한 변경 사항은 해당 클라우드 제공 Firewall Management Center 네트워크 개체 또는 그룹에 반영됩니다. 또한 **Discover & Manage Network Objects(**네트워크 개체 검색 및 관리**)**가 활성화된 각 온프레미스 방화벽 Management Center에 대한 **Devices with Pending Changes(**보류 중인 변경 사항이 있는 디바이스**)** 페이지에 항목이 생성됩니다. 여기에서 변경 사항을 선택하고 개체가 있는 온프레미스 방화벽 Management Center에 구축할 수 있습니다.

한 페이지에서 네트워크 개체 또는 그룹을 삭제하면 두 페이지 모두에서 개체 또는 그룹이 삭제됩니다.

Procedure

단계 **1** 왼쪽 창에서 개체를 클릭합니다.

단계 **2** 개체 필터 및 검색 필드를 사용하여 편집할 개체를 찾습니다.

단계 **3** 네트워크 개체를 선택하고 **Actions(**작업**)** 창에서 편집 아이콘 을 클릭합니다.

단계 **4** "Firepower 네트워크 그룹 생성"에서 생성한 것과 동일한 방식으로 대화 상자에서 값을 수정합니다.

Note
네트워크 그룹에서 개체를 제거하려면 옆에 있는 삭제 아이콘을 클릭합니다.

단계 **5** **Save(**저장**)**를 클릭합니다. Security Cloud Control는 변경의 영향을 받는 디바이스를 표시합니다.

단계 **6** **Confirm(**확인**)**을 클릭하여 개체 및 해당 개체의 영향을 받는 모든 디바이스에 대한 변경을 완료합니다.

Firepower 네트워크 그룹 편집

⚠

Caution 클라우드 제공 Firewall Management Center가 테넌트에 구축된 경우:

ASA, FDM 및 FTD 네트워크 개체 및 그룹에 대한 변경 사항은 해당 클라우드 제공 Firewall Management Center 네트워크 개체 또는 그룹에 반영됩니다. 또한 **Discover & Manage Network Objects(**네트워크 개체 검색 및 관리**)**가 활성화된 각 온프레미스 방화벽 Management Center에 대한 **Devices with Pending Changes(**보류 중인 변경 사항이 있는 디바이스**)** 페이지에 항목이 생성됩니다. 여기에서 변경 사항을 선택하고 개체가 있는 온프레미스 방화벽 Management Center에 구축할 수 있습니다.

한 페이지에서 네트워크 개체 또는 그룹을 삭제하면 두 페이지 모두에서 개체 또는 그룹이 삭제됩니다.

Procedure

단계 **1** 왼쪽 창에서 개체를 클릭합니다.

단계 **2** 개체 필터 및 검색 필드를 사용하여 편집하려는 네트워크 그룹을 찾습니다.

단계 **3** SGT 그룹을 선택하고 **Actions(**작업**)** 창에서 편집 아이콘 를 클릭합니다.

단계 **4** 필요한 경우 개체 이름과 설명을 변경합니다.

단계 **5** 이 네트워크 그룹에 새 네트워크 개체 또는 네트워크 그룹을 추가하려면 다음 단계를 수행합니다.

a. 개체 이름 또는 네트워크 그룹 옆에 나타나는 편집 아이콘 을 클릭하여 수정합니다.

b. 확인 표시를 클릭하여 변경 사항을 저장합니다. 참고: 네트워크 그룹에서 값을 제거하려면 삭제 아이콘을 클릭합니다.

단계 **6** 이 네트워크 그룹에 새 네트워크 개체 또는 네트워크 그룹을 추가하려면 다음 단계를 수행합니다.

a. **Values(**값**)** 필드에 새 값이나 기존 네트워크 개체의 이름을 입력합니다. 입력을 시작하면 Security Cloud Control에서 항목과 일치하는 개체 이름 또는 값을 제공합니다. 표시된 기존 개체 중 하나를 선택하거나 입력한 이름 또는 값을 기반으로 새 개체를 생성할 수 있습니다.

b. Security Cloud Control가 일치하는 항목을 찾은 경우 기존 개체를 선택하려면 **Add(**추가**)**를 클릭하여 네트워크 개체 또는 네트워크 그룹을 새 네트워크 그룹에 추가합니다.

c. 존재하지 않는 값 또는 개체를 입력한 경우 다음 중 하나를 수행할 수 있습니다.

- 해당 이름으로 새 개체를 생성하려면 **Add as New Object With This Name(**이 이름의 새 개체로 추가**)**을 클릭합니다. 값을 입력하고 확인 표시를 클릭하여 저장합니다.
- 새 개체를 생성하려면 **Add as New Object(**새 개체로 추가**)**를 클릭합니다. 개체 이름과 값이 동일합니다. 이름을 입력하고 확인 표시를 클릭하여 저장합니다.

값이 이미 있는 경우에도 새 개체를 생성할 수 있습니다. 이러한 개체를 변경하고 저장할 수 있습니다.

단계 **7** **Save(**저장**)**를 클릭합니다. Security Cloud Control는 변경의 영향을 받는 정책을 표시합니다.

단계 **8** **Confirm(**확인**)**을 클릭하여 개체 및 해당 개체의 영향을 받는 모든 디바이스에 대한 변경을 완료합니다.

단계 **9** 모든 디바이스에 대한 구성 변경 사항을 미리보고 구축합니다.

개체 재정의 추가

⚠

주의 클라우드 제공 Firewall Management Center가 테넌트에 구축된 경우:

ASA, FDM 및 FTD 네트워크 개체 및 그룹에 대한 변경 사항은 해당 클라우드 제공 Firewall Management Center 네트워크 개체 또는 그룹에 반영됩니다. 또한 **Discover & Manage Network Objects(**네트워크 개체 검색 및 관리**)**가 활성화된 각 온프레미스 방화벽 Management Center에 대한 **Devices with Pending Changes(**보류 중인 변경 사항이 있는 디바이스**)** 페이지에 항목이 생성됩니다. 여기에서 변경 사항을 선택하고 개체가 있는 온프레미스 방화벽 Management Center에 구축할 수 있습니다.

한 페이지에서 네트워크 개체 또는 그룹을 삭제하면 두 페이지 모두에서 개체 또는 그룹이 삭제됩니다.

프로시저

단계 **1** 왼쪽 창에서 개체를 클릭합니다.

단계 **2** 개체 필터 및 검색 필드를 사용하여 재정의를 추가할 개체를 찾습니다.

단계 **3** 네트워크 개체를 선택하고 **Actions(**작업**)** 창에서 편집 아이콘 을 클릭합니다.

단계 **4** **Override Values(**재정의 값**)** 대화 상자에 값을 입력하고 **+ Add Value(+** 값 추가**)**를 클릭합니다.

중요
추가하려는 재정의에는 개체에 포함된 것과 동일한 유형의 값이 있어야 합니다. 예를 들어 네트워크 개체에 대해 호스트 값이 아닌 네트워크 값으로만 재정의를 구성할 수 있습니다.

단계 **5** 값이 추가된 것을 확인하면, 재정의 값에서 **Devices(**디바이스**)** 열의 셀를 클릭합니다.

단계 **6** **Add Devices(**디바이스 추가**)**를 클릭하고 재정의를 추가할 디바이스를 선택합니다. 선택한 디바이스에는 재정의를 추가할 개체가 포함되어 있어야 합니다.

단계 **7** **Save(**저장**)**를 클릭합니다. Security Cloud Control는 변경의 영향을 받는 디바이스를 표시합니다.

단계 **8** **Confirm(**확인**)**을 클릭하여 개체 및 개체의 영향을 받는 모든 디바이스에 대한 재정의 추가를 완료합니다.

참고
개체에 두 개 이상의 재정의를 추가할 수 있습니다. 그러나 재정의를 추가할 때마다 개체가 포함된 다른 디바이스를 선택해야 합니다.

단계 **9** 개체 재정의에 대해 자세히 알아보고 개체 재정의 편집 , 44 페이지가 기존 재정의를 편집하려면 개체 재정의, 22 페이지을 참조하십시오.

개체 재정의 편집

개체가 디바이스에 있는 한 기존 재정의 값을 편집할 수 있습니다.

Procedure

단계 **1** 이벤트 목록을 확인하려면 개체로 이동합니다.

단계 **2** 개체 필터 및 검색 필드를 사용하여 편집하려는 재정의가 있는 개체를 찾습니다.

단계 **3** 재정의가 있는 개체를 선택하고 작업 창에서 편집 아이콘  을 클릭합니다.

단계 **4** 재정의 값을 수정합니다.

- 값을 편집하려면 편집 아이콘을 클릭합니다.
- **Override Values(**재정의 값**)**의 **Devices(**디바이스**)** 열에 있는 셀을 클릭하여 새 디바이스를 할당합니다. 이미 할당된 디바이스를 선택하고 **Remove Overrides(**재정의 제거**)**를 클릭하여 해당 디바이스에서 재정의를 제거할 수 있습니다.
- **Override Values(**재정의 값**)**에서 화살표를 클릭하여 푸시하고 공유 개체의 기본값으로 생성합니다.
- 제거하려는 재정의 옆에 있는 삭제 아이콘을 클릭합니다.

단계 **5** **Save(**저장**)**를 클릭합니다. Security Cloud Control는 변경의 영향을 받는 디바이스를 표시합니다.

단계 **6** **Confirm(**확인**)**을 클릭하여 개체 및 해당 개체의 영향을 받는 모든 디바이스에 대한 변경을 완료합니다.

단계 **7** 모든 디바이스에 대한 구성 변경 사항을 미리보고 구축합니다.

공유 네트워크 그룹에 값 추가

공유 네트워크 그룹에 연결된 모든 디바이스에 있는 값을 "기본값"이라고 합니다. Security Cloud Control은 공유 네트워크 그룹에 "추가 값"을 추가하고 해당 공유 네트워크 그룹과 연결된 일부 디바이스에 해당 값을 할당할 수 있습니다. Security Cloud Control는 변경 사항을 디바이스에 구축할 때 콘

텐츠를 확인하고 공유 네트워크 그룹과 연결된 모든 디바이스에 "기본값"을 푸시하고 지정된 디바이스에만 "추가 값"을 푸시합니다.

모든 사이트에서 액세스할 수 있어야 하는 본사에 4개의 AD 기본 서버가 있는 시나리오를 예로 들어 보겠습니다. 따라서 모든 사이트에서 사용할 "Active-Directory"라는 개체 그룹을 생성했습니다. 이제 지사 중 하나에 두 개의 AD 서버를 추가하려고 합니다. 개체 그룹 "Active-Directory"에서 해당 지사에 특정한 추가 값으로 세부 정보를 추가하여 이 작업을 수행할 수 있습니다. 이 두 서버는 "Active-Directory" 개체가 일관성이 있는지 또는 공유되는지를 확인하는 데 참여하지 않습니다. 따라서 모든 사이트에서 4개의 AD 기본 서버에 액세스할 수 있지만 지사(2개의 추가 서버 포함)는 2개의 AD 서버와 4개의 AD 기본 서버에 액세스할 수 있습니다.

Note 일치하지 않는 공유 네트워크 그룹이 있는 경우 추가 값을 사용하여 단일 공유 네트워크 그룹으로 결합할 수 있습니다. 자세한 내용은 불일치 개체 문제 해결를 참조하십시오.

Caution 클라우드 제공 Firewall Management Center가 테넌트에 구축된 경우:

ASA, FDM 및 FTD 네트워크 개체 및 그룹에 대한 변경 사항은 해당 클라우드 제공 Firewall Management Center 네트워크 개체 또는 그룹에 반영됩니다. 또한 **Discover & Manage Network Objects(**네트워크 개체 검색 및 관리**)**가 활성화된 각 온프레미스 방화벽 Management Center에 대한 **Devices with Pending Changes(**보류 중인 변경 사항이 있는 디바이스**)** 페이지에 항목이 생성됩니다. 여기에서 변경 사항을 선택하고 개체가 있는 온프레미스 방화벽 Management Center에 구축할 수 있습니다.

한 페이지에서 네트워크 개체 또는 그룹을 삭제하면 두 페이지 모두에서 개체 또는 그룹이 삭제됩니다.

Procedure

단계 **1** 왼쪽 창에서 개체를 클릭합니다.

단계 **2** 개체 필터 및 검색 필드를 사용하여 편집할 공유 네트워크 그룹을 찾습니다.

단계 **3** **Actions(**작업**)** 창에서 편집 아이콘 을 클릭합니다.

- **Devices(**디바이스**)** 필드에는 공유 네트워크 그룹이 있는 디바이스가 표시됩니다.
- **Usage(**사용**)** 필드에는 공유 네트워크 그룹과 연결된 규칙 집합이 표시됩니다.
- **Default Values(**기본값**)** 필드는 생성 중에 제공된 공유 네트워크 그룹과 연결된 기본 네트워크 개체 및 해당 값을 지정합니다. 이 필드 옆에서 이 기본값이 포함된 디바이스의 수를 볼 수 있으며, 클릭하여 해당 이름 및 디바이스 유형을 볼 수 있습니다. 이 값과 연결된 규칙 집합도 확인할 수 있습니다.

단계 **4** 추가 값 필드에 값 또는 이름을 입력합니다. 입력을 시작하면 Security Cloud Control에서 항목과 일치하는 개체 이름 또는 값을 제공합니다.

단계 **5** 표시된 기존 개체 중 하나를 선택하거나 입력한 이름 또는 값을 기반으로 새 개체를 생성할 수 있습니다.

단계 **6** Security Cloud Control가 일치하는 항목을 찾은 경우 기존 개체를 선택하려면 **Add(**추가**)**를 클릭하여 네트워크 개체 또는 네트워크 그룹을 새 네트워크 그룹에 추가합니다.

단계 **7** 존재하지 않는 값 또는 개체를 입력한 경우 다음 중 하나를 수행할 수 있습니다.

- 해당 이름으로 새 개체를 생성하려면 **Add as New Object With This Name(**이 이름의 새 개체로 추가**)**을 클릭합니다. 값을 입력하고 확인 표시를 클릭하여 저장합니다.
- 새 개체를 생성하려면 **Add as New Object(**새 개체로 추가**)**를 클릭합니다. 개체 이름과 값이 동일합니다. 이름을 입력하고 확인 표시를 클릭하여 저장합니다.

값이 이미 있는 경우에도 새 개체를 생성할 수 있습니다. 이러한 개체를 변경하고 저장할 수 있습니다.

단계 **8** **Devices(**디바이스**)** 열에서 새로 추가된 개체와 연결된 셀을 클릭하고 **Add Devices(**디바이스 추가**)**를 클릭합니다.

단계 **9** 원하는 디바이스를 선택하고 **OK(**확인**)**를 클릭합니다.

단계 **10** **Save(**저장**)**를 클릭합니다. Security Cloud Control는 변경의 영향을 받는 디바이스를 표시합니다.

단계 **11** **Confirm(**확인**)**을 클릭하여 개체 및 해당 개체의 영향을 받는 모든 디바이스에 대한 변경을 완료합니다.

단계 **12** 모든 디바이스에 대한 구성 변경 사항을 미리보고 구축합니다.

공유 네트워크 그룹의 추가 값 편집

Caution 클라우드 제공 Firewall Management Center가 테넌트에 구축된 경우:

ASA, FDM 및 FTD 네트워크 개체 및 그룹에 대한 변경 사항은 해당 클라우드 제공 Firewall Management Center 네트워크 개체 또는 그룹에 반영됩니다. 또한 **Discover & Manage Network Objects(**네트워크 개체 검색 및 관리**)**가 활성화된 각 온프레미스 방화벽 Management Center에 대한 **Devices with Pending Changes(**보류 중인 변경 사항이 있는 디바이스**)** 페이지에 항목이 생성됩니다. 여기에서 변경 사항을 선택하고 개체가 있는 온프레미스 방화벽 Management Center에 구축할 수 있습니다.

한 페이지에서 네트워크 개체 또는 그룹을 삭제하면 두 페이지 모두에서 개체 또는 그룹이 삭제됩니다.

Procedure

단계 **1** 왼쪽 창에서 개체를 클릭합니다.

단계 **2** 개체 필터 및 검색 필드를 사용하여 편집하려는 재정의가 있는 개체를 찾습니다.

단계 **3** **Actions(**작업**)** 창에서 편집 아이콘 을 클릭합니다.

단계 **4** 재정의 값을 수정합니다.

- 값을 편집하려면 편집 아이콘을 클릭합니다.
- **Devices(**디바이스**)** 열의 셀을 클릭하여 새 디바이스를 할당합니다. 이미 할당된 디바이스를 선택하고 **Remove Overrides(**재정의 제거**)**를 클릭하여 해당 디바이스에서 재정의를 제거할 수 있습니다.

- **Default Values(**기본값**)**의 화살표를 클릭하여 푸시하고 공유 네트워크 그룹의 추가 값으로 설정합니다. 공유 네트워크 그룹과 연결된 모든 디바이스가 자동으로 할당됩니다.
- **Override Values(**값 재정의**)**에서 화살표를 클릭하여 공유 네트워크 그룹의 기본 개체로 푸시하고 설정합니다.
- 네트워크 그룹에서 개체를 제거하려면 옆에 있는 삭제 아이콘을 클릭합니다.

단계 **5** **Save(**저장**)**를 클릭합니다. Security Cloud Control는 변경의 영향을 받는 디바이스를 표시합니다.

단계 **6** **Confirm(**확인**)**을 클릭하여 개체 및 해당 개체의 영향을 받는 모든 디바이스에 대한 변경을 완료합니다.

단계 **7** 모든 디바이스에 대한 구성 변경 사항을 미리보고 구축합니다.

Security Cloud Control에서 네트워크 개체 및 그룹 삭제

클라우드 제공 Firewall Management Center가 테넌트에 구축된 경우:

개체 페이지에서 네트워크 개체 또는 그룹을 삭제하면 클라우드 제공 Firewall Management Center의 개체 페이지에서 복제된 네트워크 개체 또는 그룹이 삭제되며, 그 반대의 경우도 마찬가지입니다.

온프레미스 **Firewall Management Center** 네트워크 개체 검색 및 관리

Security Cloud Control를 사용하여 관리하는 온프레미스 방화벽 Management Center가 있고 해당 개체를 공유하고 관리하려면 다음을 수행합니다.

프로시저

단계 **1** 왼쪽 창에서 **Administration(**관리**)** > **Integration(**통합**)** > **Firewall Management Center**를 선택하여 **Services(**서비스**)** 페이지를 확인합니다.

단계 **2** 온프레미스 방화벽 Management Center를 이미 Security Cloud Control에 온보딩한 경우, 이를 선택합니다.

새 온프레미스 방화벽 Management Center를 온보딩하려면 온프레미스 Firewall Management Center 온보딩을 참조하십시오.

단계 **3** 오른쪽의 **Actions(**작업**)** 창에서 **Settings(**설정**)**를 선택합니다. 둘 이상의 온프레미스 방화벽 Management Center를 선택하는 경우에는 **Actions(**작업**)** 창이 표시되지 않습니다.

참고
관리자 또는 최고 관리자여야 **Settings(**설정**)**를 사용할 수 있습니다.

단계 **4** **Discover & Manage Network Objects(**네트워크 개체 검색 및 관리**)** 토글 버튼을 활성화합니다.변경 사항을 검토를 위해 스테이징하지 않고 온프레미스 방화벽 Management Center과 자동으로 동기화하려면 네트워크 개체의 자동 동기화 사용 토글을 활성화합니다.

참고
- 선택한 온프레미스 방화벽 Management Center에 하나 이상의 하위 도메인이 있거나 변경 관리 워크플로우가 활성화되어 있는 경우에는 **Discover & Manage Network Objects(**네트워크 개체 검색 및 관리**)** 토글을 켤 수 없습니다.

- **Discover & Manage Network Objects(**네트워크 개체 검색 및 관리**)** 토글이 꺼져 있으면 **Enable automatic sync of network objects(**네트워크 개체 자동 동기화 활성화**)** 토글을 켤 수 없습니다.

Security Cloud Control에 온보딩되는 모든 새 온프레미스 방화벽 Management Center에 대해 이 토글 버튼은 수동으로 활성화해야 합니다. 이 옵션을 활성화하면 Security Cloud Control는 온프레미스 방화벽 Management Center에서 개체 검색을 시작합니다. 이러한 개체는 공유, 관리, Security Cloud Control에서 관리하는 다른 플랫폼 전반에서 일관된 개체 정의를 설정하는 데 사용할 수 있습니다.

Security Cloud Control에서 온프레미스 방화벽 Management Center에서 검색된 개체에 재정의를 추가하고 변경 사항을 온프레미스 방화벽 Management Center로 다시 푸시하면 이러한 개체는 이전에는 재정의를 허용하지 않았더라도 온프레미스 방화벽 Management Center에서 재정의를 수락하기 시작합니다. Security Cloud Control에서 재정의가 추가되는 경우 **View Network Object(**네트워크 개체 보기**)** 창의 **Allow Overrides(**재정의 허용**)** 확인란이 자동으로 선택됩니다.

참고
Security Cloud Control의 이미 존재하는 개체를 온프레미스 방화벽 Management Center에 할당하려면 온프레미스 방화벽 Management Center를 선택하고 **Actions(**작업**)** 창에서 **Assign Objects(**개체 할당**)**를 클릭합니다.

관련 정보

- 네트워크 개체
- 온프레미스 Firewall Management Center 구성 미리보기 및 구축
- 온프레미스 방화벽 Management Center에서 충돌 탐지 활성화

서비스 개체

프로토콜 개체

프로토콜 개체는 덜 일반적으로 사용되는 또는 레거시 프로토콜을 포함하는 서비스 개체 유형입니다. 프로토콜 개체는 이름과 프로토콜 번호로 식별됩니다. Security Cloud Control는 ASA 및 Firepower(FDM 관리 디바이스) 구성에서 이러한 개체를 인식하고 사용자가 쉽게 찾을 수 있도록 자체 필터인 "프로토콜"을 제공합니다.

ICMP 개체

ICMP(인터넷 제어 메시지 프로토콜) 개체는 ICMP 및 IPv6-ICMP 메시지 전용 서비스 개체입니다. Security Cloud Control는 ASA 및 Firepower 구성에서 해당 디바이스가 온보딩되었을 때 이러한 개체를 인식하고 Security Cloud Control는 사용자가 개체를 쉽게 찾을 수 있도록 해당 디바이스에 "ICMP" 필터를 제공합니다.

Security Cloud Control를 사용하면 ASA 구성에서 ICMP 개체를 제거하거나 이름을 바꿀 수 있습니다. Security Cloud Control를 사용하여 Firepower 구성에서 ICMP 및 ICMPv6 개체를 생성, 업데이트 및 삭제할 수 있습니다.

Note ICMPv6 프로토콜의 경우 AWS는 특정 인수 선택을 지원하지 않습니다. 모든 ICMPv6 메시지를 허용하는 규칙만 지원됩니다.

관련 정보:

• 개체 삭제, on page 28

네트워크 주소 변환

IP 네트워크 내의 각 컴퓨터와 디바이스에는 호스트를 식별하는 고유한 IP 주소가 할당됩니다. 공용 IPv4 주소의 부족 때문에 이러한 IP 주소는 대부분 사설이며, 사설 회사 네트워크 외부로 라우팅되지 않습니다. RFC 1918의 정의에 따르면 사설 IP 주소는 내부적으로 사용할 수 있지만 외부에 알려서는 안 되는 주소입니다.

- 10.0.0.0~10.255.255.255
- 172.16.0.0 ~ 172.31.255.255
- 192.168.0.0~192.168.255.255

NAT의 주요 기능 중 하나는 사설 IP 네트워크가 인터넷에 연결되도록 하는 것입니다. NAT는 사설 IP 주소를 공용 IP 주소로 교체하여, 내부 사설 네트워크의 사설 주소를 공용 인터넷에서 사용할 수 있는 합법적이고 라우팅 가능한 주소로 전환합니다. 이렇게 하여 NAT는 공용 주소를 절약합니다. 전체 네트워크에 대해 최소 하나의 공용 주소만 외부에 알리도록 구성할 수 있기 때문입니다.

NAT의 기타 기능은 다음과 같습니다.

- 보안 - 직접 공격을 피할 수 있도록 내부 IP 주소를 숨깁니다.
- IP 라우팅 솔루션 - NAT를 사용하는 경우 중첩 IP 주소 문제가 발생하지 않습니다.
- 유연성 - 외부적으로 사용 가능한 공용 주소에 영향을 주지 않고 내부 IP 주소 지정 방식을 변경할 수 있습니다. 예를 들어 인터넷에 액세스할 수 있는 서버의 경우, 인터넷용으로는 고정 IP 주소를 유지하고 내부적으로는 서버 주소를 변경할 수 있습니다.
- IPv4와 IPv6 간 변환(라우팅된 방식 전용) - IPv6 네트워크를 IPv4 네트워크에 연결하려는 경우 NAT를 이용하면 두 가지 주소 유형 간에 변환할 수 있습니다.

Security Cloud Control을 사용하여 다양한 활용 사례에 대한 NAT 규칙을 생성할 수 있습니다. NAT 규칙 마법사 또는 다음 항목을 사용하여 다른 NAT 규칙을 생성합니다.

NAT 규칙 처리 순서

네트워크 개체 NAT 규칙과 2회 NAT 규칙은 세 개의 섹션으로 구분되는 단일 테이블에 저장됩니다. 섹션 1 규칙이 먼저 적용된 다음, 일치가 발견될 때까지 섹션 2, 마지막으로 섹션 3이 적용됩니다. 예

를 들어 섹션 1에서 일치가 발견되면 섹션 2와 3은 평가되지 않습니다. 다음 표는 각 섹션 내의 규칙 순서를 보여줍니다.

Table 5: NAT 규칙 테이블

테이블 섹션	규칙 유형	섹션 내 규칙의 순서
섹션 1	2회 NAT(ASA) 수동 NAT(FTD)	첫 번째 일치부터 구성에 나타나는 순서대로 적용됩니다. 첫 번째 일치가 적용되므로, 일반 규칙 앞에 특수 규칙이 오도록 해야 합니다. 그렇지 않으면 특수 규칙이 원하는 대로 적용되지 않을 수 있습니다. 기본적으로 2회 NAT 규칙은 섹션 1에 추가됩니다.
섹션 2	네트워크 개체 NAT(ASA) 자동 NAT(FTD)	섹션 1에서 일치하는 항목을 찾을 수 없으면 섹션 2 규칙이 다음 순서로 적용됩니다. **1.** 고정 규칙 **2.** 동적 규칙 각 규칙 유형 내에서는 다음의 순서 지침이 사용됩니다**.** **1.** 실제 IP 주소의 수량 - 가장 적은 것에서 가장 많은 것. 예를 들면 주소가 1개인 개체가 주소가 10개인 개체보다 먼저 평가됩니다. **2.** 수량이 동일한 경우 IP 주소 번호가 낮은 것에서 높은 것 순으로 사용됩니다. 예를 들면, 10.1.1.0이 11.1.1.0보다 먼저 평가됩니다. **3.** IP 주소가 동일한 경우 네트워크 개체의 이름이 알파벳순으로 사용됩니다. 예를 들어 "Arlington" 개체는 "Detroit" 개체보다 먼저 평가됩니다.
섹션 3	2회 NAT(ASA) 수동 NAT(FTD)	아직도 일치가 발견되지 않으면 섹션 3 규칙이 첫 번째부터 구성에 나타나는 순서대로 적용됩니다. 이 섹션에는 가장 일반적인 규칙을 포함해야 합니다. 또한 이 섹션에서는 특정 규칙이 일반 규칙보다 먼저 적용되도록 해야 합니다.

예를 들어 섹션 2 규칙의 경우 네트워크 개체 내에서 다음 IP 주소를 정의합니다.

- 192.168.1.0/24(고정)
- 192.168.1.0/24(동적)
- 10.1.1.0/24(고정)

- 192.168.1.1/32(고정)
- 172.16.1.0/24(동적) (개체 Detroit)
- 172.16.1.0/24(동적)(개체 Arlington)

결과 순서는 다음과 같습니다.

- 192.168.1.1/32(고정)
- 10.1.1.0/24(고정)
- 192.168.1.0/24(고정)
- 172.16.1.0/24(동적)(개체 Arlington)
- 172.16.1.0/24(동적) (개체 Detroit)
- 192.168.1.0/24(동적)

네트워크 주소 변환 마법사

NAT(Network Address Translation) 마법사는 다음 유형의 액세스에 대해 디바이스에서 NAT 규칙을 만드는 데 도움이 됩니다.

- 내부 사용자의 인터넷 액세스를 활성화합니다. 이 NAT 규칙을 사용하여 내부 네트워크의 사용자가 인터넷에 연결할 수 있습니다.
- 내부 서버를 인터넷에 노출합니다. 이 NAT 규칙을 사용하여 네트워크 외부의 사람들이 내부 웹 또는 이메일 서버에 도달하도록 허용할 수 있습니다.

"내부 사용자를 위한 인터넷 액세스 활성화**"**의 전제 조건

NAT 규칙을 생성하기 전에 다음 정보를 수집하십시오.

- 사용자에게 가장 가까운 인터페이스 이것은 일반적으로 "내부" 인터페이스라고 합니다.
- 인터넷 연결에 가장 가까운 인터페이스 이것은 일반적으로 "외부" 인터페이스라고 합니다.
- 특정 사용자만 인터넷에 연결할 수 있도록 하려면 해당 사용자의 서브넷 주소가 필요합니다.

"내부 서버를 인터넷에 노출**"**하기 위한 전제 조건

NAT 규칙을 생성하기 전에 다음 정보를 수집하십시오.

- 사용자에게 가장 가까운 인터페이스 이것은 일반적으로 "내부" 인터페이스라고 합니다.
- 인터넷 연결에 가장 가까운 인터페이스 이것은 일반적으로 "외부" 인터페이스라고 합니다.
- 인터넷 연결 IP 주소로 변환하려는 네트워크 내부 서버의 IP 주소입니다.
- 서버에서 사용할 공용 IP 주소입니다.

다음 작업

NAT 마법사를 사용하여 NAT 규칙 생성, on page 52의 내용을 참조하십시오.

NAT 마법사를 사용하여 NAT 규칙 생성

Before you begin

NAT 마법사를 사용하여 NAT 규칙을 만드는 데 필요한 사전 요구 사항은 네트워크 주소 변환 마법사, on page 51를 참조하십시오.

Procedure

단계 **1** 왼쪽 창에서 보안 디바이스를 클릭합니다.

단계 **2** **Devices(**디바이스**)** 탭을 클릭하여 디바이스를 찾거나 **Templates(**템플릿**)** 탭을 클릭하여 모델 디바이스를 찾습니다.

단계 **3** 해당 디바이스 탭을 클릭합니다.

단계 **4** Filter(필터) 및 Search(검색) 필드를 사용하여 NAT 규칙을 생성하려는 디바이스를 찾으십시오.

단계 **5** 상세정보 패널의 **Management(**관리**)** 영역에서 **NAT** NAT를 클릭합니다.

단계 **6**  > **NAT Wizard(NAT** 마법사**)**를 클릭합니다.

단계 **7** NAT 마법사 질문에 응답하고 화면의 지시를 따르십시오.

- NAT 마법사는 네트워크 개체, on page 29를 사용하여 규칙을 생성합니다. 드롭다운 메뉴에서 기존 개체를 선택하거나 만들기 버튼  를 사용하여 새 개체를 생성합니다.
- NAT 규칙을 저장하려면 먼저 모든 IP 주소를 네트워크 개체로 정의해야 합니다.

단계 **8** 지금 변경 사항을 검토하고 구축하거나 기다렸다가 여러 변경 사항을 한 번에 구축합니다.

NAT의 일반적인 사용 사례

2회 NAT 및 수동 NAT

다음은 "자동 NAT"라고도 하는 "네트워크 개체 NAT"를 사용하여 수행할 수 있는 몇 가지 일반적인 작업입니다.

- 공용 IP 주소를 사용하여 인터넷에 연결하도록 내부 네트워크의 서버 활성화, 53 페이지
- 내부 네트워크의 사용자가 외부 인터페이스의 공용 IP 주소를 사용하여 인터넷에 액세스하도록 활성화, 54 페이지
- 공용 IP 주소의 특정 포트에서 내부 네트워크의 서버를 사용할 수 있도록 설정, 55 페이지

• 사설 IP 주소 범위를 공용 IP 주소 범위로 변환, 58 페이지

네트워크 개체 및 **NAT**자동 **NAT**

다음은 "수동 NAT"라고도 하는 "Twice NAT"를 사용하여 수행할 수 있는 일반적인 작업입니다.

• 외부 인터페이스를 통과할 때 IP 주소 범위가 변환되지 않도록 방지, 60 페이지

공용 IP 주소를 사용하여 인터넷에 연결하도록 내부 네트워크의 서버 활성화

활용 사례

인터넷에서 액세스해야 하는 사설 IP 주소가 있는 서버가 있고 사설 IP 주소에 대해 하나의 공용 IP 주소를 NAT하기에 충분한 공용 IP 주소가 있는 경우 이 NAT 전략을 사용합니다. 공용 IP 주소가 제한된 경우 공용 IP 주소의 특정 포트에서 사용자가 사용할 수 있는 내부 네트워크의 서버 만들기를 참조하세요(해당 솔루션이 더 적합할 수 있음).

전략

서버에는 정적 사설 IP 주소가 있으며 네트워크 외부의 사용자는 서버에 연결할 수 있어야 합니다. 고정 사설 IP 주소를 고정 공용 IP 주소로 변환하는 네트워크 개체 NAT 규칙을 생성합니다. 그런 다음 해당 공용 IP 주소에서 사설 IP 주소에 도달하는 트래픽을 허용하는 액세스 정책을 생성합니다. 마지막으로 이러한 변경 사항을 디바이스에 구축합니다.

Before you begin

시작하기 전에 두 개의 네트워크 개체를 생성합니다. 하나의 개체는 *servername_inside*로 이름을 지정하고 다른 개체는 *servername_outside*로 이름을 지정합니다. *servername*_inside 네트워크 개체는 서버의 사설 IP 주소를 포함해야 합니다. *servername*_outside 네트워크 개체에는 서버의 공용 IP 주소가 포함되어야 합니다.

지침은 네트워크 개체 생성을 참조하십시오.

Procedure

단계 **1** 왼쪽 창에서 보안 디바이스를 클릭합니다.

단계 **2** **Devices(**디바이스**)** 탭을 클릭하여 디바이스를 찾거나 **Templates(**템플릿**)** 탭을 클릭하여 모델 디바이스를 찾습니다.

단계 **3** 해당 디바이스 탭을 클릭합니다.

단계 **4** NAT 규칙을 생성하려는 디바이스를 선택합니다.

단계 **5** 오른쪽의 **Management(**관리**)** 창에서 **NAT**를 클릭합니다.

단계 **6**  > **Network Object NAT**를 클릭합니다.

단계 **7** 섹션 1, **Type(**유형**)**에서 **Static(**정적**)**을 선택합니다. **Continue(**계속**)**를 클릭합니다.

단계 **8** 섹션 2, **Interfaces(**인터페이스**)**에서 소스 인터페이스로 **inside(**내부**)**를 선택하고 대상 인터페이스로 **outside(**외부**)**를 선택합니다. **Continue(**계속**)**를 클릭합니다.

단계 **9** 섹션 3, **Packets(**패킷**)**에서 , 다음 작업을 수행합니다.

a. 원본 주소 메뉴를 확장하고 **Choose(**선택**)**을 클릭한 다음 **servername_inside** 개체를 선택합니다.

b. 변환된 주소 메뉴를 확장하고 **Choose(**선택**)**을 클릭한 다음 **servername_outside** 개체를 선택합니다.

단계 **10** 섹션 4, **Advanced(**고급**)**을 건너뜁니다.

단계 **11** FDM 매니지드 디바이스의 경우 섹션 5, 이름에서 NAT 규칙에 이름을 지정합니다.

단계 **12** **Save(**저장**)**를 클릭합니다.

단계 **13** ASA의 경우 네트워크 정책 규칙을 구축하거나 기다렸다가, FDM 관리 디바이스의 경우 액세스 제어 정책 규칙을 구축하여 트래픽이 *servername*_inside에서 *servername*_outside로 흐를 수 있도록 합니다.

단계 **14** 지금 변경 사항을 검토하고 구축하거나 기다렸다가 여러 변경 사항을 한 번에 구축합니다.

내부 네트워크의 사용자가 외부 인터페이스의 공용 IP 주소를 사용하여 인터넷에 액세스하도록 활성화

활용 사례

외부 인터페이스의 공용 주소를 공유하여 개인 네트워크의 사용자와 컴퓨터가 인터넷에 연결할 수 있도록 합니다.

전략

사설 네트워크의 모든 사용자가 디바이스의 외부 인터페이스 공용 IP 주소를 공유할 수 있도록 허용하는 포트 주소 변환(PAT) 규칙을 생성합니다.

사설 주소가 공용 주소 및 포트 번호에 매핑된 후 디바이스는 해당 매핑을 기록합니다. 해당 공용 IP 주소 및 포트로 향하는 들어오는 트래픽이 수신되면 디바이스는 이를 요청한 사설 IP 주소로 다시 보냅니다.

Procedure

단계 **1** 왼쪽 창에서 보안 디바이스를 클릭합니다.

단계 **2** **Devices(**디바이스**)** 탭을 클릭하여 디바이스를 찾거나 **Templates(**템플릿**)** 탭을 클릭하여 모델 디바이스를 찾습니다.

단계 **3** 해당 디바이스 탭을 클릭합니다.

단계 **4** NAT 규칙을 생성하려는 디바이스를 선택합니다.

단계 **5** 오른쪽의 **Management(**관리**)** 창에서 **NAT**를 클릭합니다.

단계 **6**  > **Network Object NAT**를 클릭합니다.

단계 **7** 섹션 1, 유형 에서 **Dynamic(**동적**)**을 선택합니다. **Continue(**계속**)**를 클릭합니다.

단계 **8** 섹션 2, 인터페이스에서, 소스 인터페이스로 **any(**아무거나**)**를 선택하고 대상 인터페이스로 **outside(**외부**)**를 선택합니다. **Continue(**계속**)**를 클릭합니다.

단계 **9** 섹션 3, **Packets(**패킷**)**에서, 다음 작업을 수행합니다.

a. 원래 주소 메뉴를 확장하고, **Choose(**선택**)**을 클릭한 다음 네트워크 구성에 따라 **any-ipv4** 또는 **any-ipv6** 개체를 선택합니다.

b. 변환된 주소 메뉴를 확장하고 사용 가능한 목록에서 인터페이스를 선택합니다. 인터페이스는 외부 인터페이스의 공용 주소를 사용하도록 나타냅니다.

단계 **10** FDM 매니지드 디바이스의 경우 섹션 5, 이름에서 NAT 규칙의 이름을 입력합니다.

단계 **11** **Save(**저장**)**를 클릭합니다.

단계 **12** 지금 변경 사항을 검토하고 구축하거나 기다렸다가 여러 변경 사항을 한 번에 구축합니다.

ASA의 저장된 구성 파일 항목

다음은 이 절차의 결과로 생성되어 ASA의 저장된 구성 파일에 나타나는 항목입니다.

Note 이것은 FDM 관리 디바이스에 적용되지 않습니다.

이 절차에 의해 생성된 개체

```
object network any_network
subnet 0.0.0.0 0.0.0.0
```

이 절차에 의해 생성된 ***NAT*** 규칙

```
object network any_network
nat (any,outside) dynamic interface
```

공용 IP 주소의 특정 포트에서 내부 네트워크의 서버를 사용할 수 있도록 설정

활용 사례

공용 IP 주소가 하나만 있거나 매우 제한된 수인 경우, 정적 IP 주소 및 포트에 바인딩된 인바운드 트래픽을 내부 주소로 변환하는 네트워크 개체 NAT 규칙을 만들 수 있습니다. 특정 사례에 대한 절차를 제공했지만 지원되는 다른 애플리케이션의 모델로 사용할 수 있습니다.

사전 요구 사항

시작하기 전에 FTP, HTTP 및 SMTP 서버에 각각 하나씩 세 개의 개별 네트워크 개체를 생성합니다. 다음 절차를 위해 이러한 개체를 **ftp-server-object**, **http-server-object** 및 **smtp-server-object**라고 합니다.

지침은 을 참조하십시오.

FTP 서버에 대한 NAT 수신 FTP 트래픽

Procedure

단계 1 왼쪽 창에서 보안 디바이스를 클릭합니다.

단계 2 **Devices(**디바이스**)** 탭을 클릭하여 디바이스를 찾거나 **Templates(**템플릿**)** 탭을 클릭하여 모델 디바이스를 찾습니다.

단계 3 해당 디바이스 탭을 클릭합니다.

단계 4 NAT 규칙을 생성하려는 디바이스를 선택합니다.

단계 5 오른쪽의 **Management(**관리**)** 창에서 **NAT**를 클릭합니다.

단계 6  > **Network Object NAT**를 클릭합니다.

단계 7 섹션 1, **Type(**유형**)**에서 **Static(**정적**)**을 선택합니다. **Continue(**계속**)**를 클릭합니다.

단계 8 섹션 2, **Interfaces(**인터페이스**)**에서 소스 인터페이스로 **inside(**내부**)**를 선택하고 대상 인터페이스로 **outside(**외부**)**를 선택합니다. **Continue(**계속**)**를 클릭합니다.

단계 9 섹션 3, **Packets(**패킷**)**에서 , 다음 작업을 수행합니다.

- 원본 주소 메뉴를 확장하고, **Choose(**선택**)**를 클릭한 다음**ftp**-server-object를 선택합니다.
- 변환된 주소 메뉴를 확장하고, **Choose(**선택**)**를 클릭한 다음 **Interface(**인터페이스**)**를 선택합니다.
- **Use Port Translation(**포트 변환 사용**)**을 선택합니다.
- **tcp**, **ftp, ftp**를 선택합니다.

단계 10 섹션 4, **Advanced(**고급**)**을 건너뜁니다.

단계 11 FDM 매니지드 디바이스의 경우 섹션 5, 이름에서 NAT 규칙에 이름을 지정합니다.

단계 12 **Save(**저장**)**를 클릭합니다. NAT 테이블의 섹션 2에 새 규칙이 생성됩니다.

단계 13 지금 변경 사항을 검토하고 구축하거나 기다렸다가 여러 변경 사항을 한 번에 구축합니다.

HTTP 서버에 대한 NAT 수신 HTTP 트래픽

공용 IP 주소가 하나만 있거나 매우 제한된 수인 경우, 정적 IP 주소 및 포트에 바인딩된 인바운드 트래픽을 내부 주소로 변환하는 네트워크 개체 NAT 규칙을 만들 수 있습니다. 특정 사례에 대한 절차를 제공했지만 지원되는 다른 애플리케이션의 모델로 사용할 수 있습니다.

Before you begin

시작하기 전에 http 서버에 대한 네트워크 개체를 생성합니다. 이 절차에서는개체를 **http-object**라고 합니다.

지침은 을 참조하십시오.

Procedure

단계 **1** 왼쪽 창에서 보안 디바이스를 클릭합니다.

단계 **2** **Devices(**디바이스**)** 탭을 클릭하여 디바이스를 찾거나 **Templates(**템플릿**)** 탭을 클릭하여 모델 디바이스를 찾습니다.

단계 **3** 해당 디바이스 탭을 클릭합니다.

단계 **4** NAT 규칙을 생성하려는 디바이스를 선택합니다.

단계 **5** 오른쪽의 **Management(**관리**)** 창에서 **NAT**를 클릭합니다.

단계 **6** + **> Network Object NAT**를 클릭합니다.

단계 **7** 섹션 1, **Type(**유형**)**에서 **Static(**정적**)**을 선택합니다. **Continue(**계속**)**를 클릭합니다.

단계 **8** 섹션 2, **Interfaces(**인터페이스**)**에서 소스 인터페이스로 **inside(**내부**)**를 선택하고 대상 인터페이스로 **outside(**외부**)**를 선택합니다. **Continue(**계속**)**를 클릭합니다.

단계 **9** 섹션 3, **Packets(**패킷**)**에서 , 다음 작업을 수행합니다.

- 원본 주소 메뉴를 확장하고 **Choose(**선택**)**을 클릭한 다음 **http**-object를 선택합니다.
- 변환된 주소 메뉴를 확장하고, **Choose(**선택**)**를 클릭한 다음 **Interface(**인터페이스**)**를 선택합니다.
- **Use Port Translation(**포트 변환 사용**)**을 선택합니다.
- **tcp**, **http**, http를 선택합니다.

단계 **10** 섹션 4, **Advanced(**고급**)**을 건너뜁니다.

단계 **11** FDM 매니지드 디바이스의 경우 섹션 5, 이름에서 NAT 규칙에 이름을 지정합니다.

단계 **12** **Save(**저장**)**를 클릭합니다. NAT 테이블의 섹션 2에 새 규칙이 생성됩니다.

단계 **13** 지금 변경 사항을 검토하고 구축하거나 기다렸다가 여러 변경 사항을 한 번에 구축합니다.

SMTP 서버에 대한 NAT 수신 SMTP 트래픽

공용 IP 주소가 하나만 있거나 매우 제한된 수인 경우, 정적 IP 주소 및 포트에 바인딩된 인바운드 트래픽을 내부 주소로 변환하는 네트워크 개체 NAT 규칙을 만들 수 있습니다. 특정 사례에 대한 절차를 제공했지만 지원되는 다른 애플리케이션의 모델로 사용할 수 있습니다.

Before you begin

시작하기 전에 smtp 서버에 대한 네트워크 개체를 생성합니다. 이 절차에서는개체를 **smtp**-개체라고 합니다.

지침은 을 참조하십시오.

Procedure

단계 **1** 왼쪽 창에서 보안 디바이스를 클릭합니다.

단계 **2** **Devices(**디바이스**)** 탭을 클릭하여 디바이스를 찾거나 **Templates(**템플릿**)** 탭을 클릭하여 모델 디바이스를 찾습니다.

단계 **3** 해당 디바이스 탭을 클릭합니다.

단계 **4** NAT 규칙을 생성하려는 디바이스를 선택합니다.

단계 **5** 오른쪽의 **Management(**관리**)** 창에서 **NAT**를 클릭합니다.

단계 **6**  **> Network Object NAT**를 클릭합니다.

단계 **7** 섹션 1, **Type(**유형**)**에서 **Static(**정적**)**을 선택합니다. **Continue(**계속**)**를 클릭합니다.

단계 **8** 섹션 2, **Interfaces(**인터페이스**)**에서 소스 인터페이스로 **inside(**내부**)**를 선택하고 대상 인터페이스로 **outside(**외부**)**를 선택합니다. **Continue(**계속**)**를 클릭합니다.

단계 **9** 섹션 3, **Packets(**패킷**)**에서 , 다음 작업을 수행합니다.

- 원본 주소 메뉴를 확장하고, **Choose(**선택**)**를 클릭한 다음 smtp-server-object를 선택합니다.
- 변환된 주소 메뉴를 확장하고, **Choose(**선택**)**를 클릭한 다음 **Interface(**인터페이스**)**를 선택합니다.
- **Use Port Translation(**포트 변환 사용**)**을 선택합니다.
- **tcp**, **smtp**, **smtp**를 선택합니다.

단계 **10** 섹션 4, **Advanced(**고급**)**을 건너뜁니다.

단계 **11** FDM 매니지드 디바이스의 경우 섹션 5, 이름에서 NAT 규칙에 이름을 지정합니다.

단계 **12** **Save(**저장**)**를 클릭합니다. NAT 테이블의 섹션 2에 새 규칙이 생성됩니다.

단계 **13** 지금 변경 사항을 검토하고 구축하거나 기다렸다가 여러 변경 사항을 한 번에 구축합니다.

사설 IP 주소 범위를 공용 IP 주소 범위로 변환

활용 사례

수신 디바이스(트랜잭션의 다른 끝에 있는 디바이스)가 트래픽을 허용하도록 IP 주소를 특정 범위로 변환해야 하는 특정 디바이스 유형 또는 사용자 유형 그룹이 있는 경우 이 접근 방식을 사용합니다.

내부 주소 풀을 외부 주소 풀로 변환

Before you begin

변환하려는 사설 IP 주소 풀에 대한 네트워크 개체를 생성하고 해당 사설 IP 주소를 변환하려는 공용 주소 풀에 대한 네트워크 개체를 생성합니다.

Note ASA 의 경우 "변환된 주소" 풀을 정의하는 네트워크 그룹은 서브넷을 정의하는 네트워크 개체일 수 없습니다.

이러한 주소 풀을 생성할 때 지침을 보려면 하고 하십시오.

다음 절차를 위해 개인 주소 풀의 이름을 **inside_pool**로 지정하고 공용 주소 풀의 이름을 **outside_pool**로 지정했습니다.

Procedure

단계 **1** 왼쪽 창에서 보안 디바이스를 클릭합니다.

단계 **2** **Devices(**디바이스**)** 탭을 클릭하여 디바이스를 찾거나 **Templates(**템플릿**)** 탭을 클릭하여 모델 디바이스를 찾습니다.

단계 **3** 해당 디바이스 탭을 클릭합니다.

단계 **4** NAT 규칙을 생성하려는 디바이스를 선택합니다.

단계 **5** 오른쪽의 **Management(**관리**)** 창에서 **NAT**를 클릭합니다.

단계 **6** + **> Network Object NAT**를 클릭합니다.

단계 **7** 섹션 1 **Type(**유형**)**에서 **Dynamic(**동적**)**을 선택하고 **Continue(**계속**)**를 클릭합니다.

단계 **8** 섹션 2, 인터페이스에서 소스 인터페이스를 내부로, 대상 인터페이스를 외부로 설정합니다. **Continue(**계속**)**를 클릭합니다.

단계 **9** 섹션 3, **Packets(**패킷**)**에서, 다음 작업을 수행합니다.

- 원본 주소의 경우 **Choose(**선택**)**을 클릭한 다음 위의 전제 조건 섹션에서 만든 **inside_pool** 네트워크 개체(또는 네트워크 그룹)를 선택합니다.
- 변환된 주소의 경우 **Choose(**선택**)**을 클릭한 다음 위의 전제 조건 섹션에서 만든 **outside_pool** 네트워크 개체(또는 네트워크 그룹)를 선택합니다.

단계 **10** 섹션 4, **Advanced(**고급**)**을 건너뜁니다.

단계 **11** FDM 매니지드 디바이스의 경우 섹션 5, 이름에서 NAT 규칙에 이름을 지정합니다.

단계 **12** **Save(**저장**)**를 클릭합니다.

단계 **13** 지금 변경 사항을 검토하고 구축하거나 기다렸다가 여러 변경 사항을 한 번에 구축합니다.

외부 인터페이스를 통과할 때 IP 주소 범위가 변환되지 않도록 방지

활용 사례

이 Twice NAT 사용 사례를 사용하여 사이트 간 VPN을 활성화합니다.

전략

네트워크의 한 위치에 있는 IP 주소가 다른 위치에 변경되지 않고 도착하도록 IP 주소 풀을 자체적으로 변환하고 있습니다.

2회 NAT 규칙 생성

Before you begin

변환할 IP 주소 풀을 정의하는 네트워크 개체 또는 네트워크 그룹을 생성합니다. ASA의 경우 주소 범위는 IP 주소 범위를 사용하는 네트워크 개체, 서브넷을 정의하는 네트워크 개체 또는 범위의 모든 주소를 포함하는 네트워크 그룹 개체로 정의할 수 있습니다.

네트워크 개체 또는 네트워크 그룹을 생성할 때 지침을 보려면 을 사용합니다.

다음 절차를 위해 네트워크 개체 또는 네트워크 그룹인 Site-to-Site-PC-Pool을 호출합니다.

Procedure

단계 **1** 왼쪽 창에서 보안 디바이스를 클릭합니다.

단계 **2** **Devices(**디바이스**)** 탭을 클릭하여 디바이스를 찾거나 **Templates(**템플릿**)** 탭을 클릭하여 모델 디바이스를 찾습니다.

단계 **3** 해당 디바이스 탭을 클릭합니다.

단계 **4** NAT 규칙을 생성하려는 디바이스를 선택합니다.

단계 **5** 오른쪽의 **Management(**관리**)** 창에서 **NAT**를 클릭합니다.

단계 **6**  > **Twice NAT(2**회 **NAT)**를 클릭합니다..

단계 **7** 섹션 1, **Type(**유형**)**에서 **Static(**정적**)**을 선택합니다. **Continue(**계속**)**를 클릭합니다.

단계 **8** 섹션 2, **Interfaces(**인터페이스**)**에서 소스 인터페이스로 **inside(**내부**)**를 선택하고 대상 인터페이스로 **outside(**외부**)**를 선택합니다. **Continue(**계속**)**를 클릭합니다.

단계 **9** 섹션 3, 패킷에서 다음과 같이 변경합니다.

- 원래 주소 메뉴를 확장하고 **Choose(**선택**)**를 클릭한 다음 전제 조건 섹션에서 생성한 사이트 간 PC 풀 개체를 선택합니다.
- 변환된 주소 메뉴를 펼치고 **Choose(**선택**)**를 클릭한 후 전제 조건 섹션에서 생성한 Site-to-Site-PC-Pool 개체를 선택합니다.

단계 **10** 섹션 4, **Advanced(**고급**)**을 건너뜁니다.

단계 **11** FDM 매니지드 디바이스의 경우 섹션 5, 이름에서 NAT 규칙에 이름을 지정합니다.

단계 **12** **Save(**저장**)**를 클릭합니다.

단계 **13** ASA의 경우 암호화 맵을 생성합니다. 암호화 맵 생성에 대한 자세한 내용은 CLI 책 3: Cisco ASA Series VPN CLI 구성 가이드를 참조하고 LAN-to-LAN IPsec VPN에 대한 장을 검토하십시오.

단계 **14** 지금 변경 사항을 검토하고 구축하거나 기다렸다가 여러 변경 사항을 한 번에 구축합니다.

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.

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.