개체 관리

이 장에서는 재사용 가능한 개체를 관리하는 방법을 설명합니다.

개체 소개

향상된 유연성 및 웹 인터페이스 사용 편의성을 위해 Firepower System은 이름과 값을 연결하는 재사용 가능한 설정으로 명명된 개체를 사용합니다. 해당 값을 사용하려는 경우 명명된 개체를 사용합니다. 시스템은 다양한 정책 및 규칙, 이벤트 검색, 보고서, 대시보드 등을 포함해 웹 인터페이스의 다양한 위치에서 개체 사용을 지원합니다. 시스템은 자주 사용된 설정을 대표하는 여러 개의 사전 정의된 개체를 제공합니다.

개체 관리자를 사용하여 개체를 생성하고 관리합니다. 개체를 사용하는 많은 설정도 즉석에서 필요에 따라 개체를 생성할 수 있도록 합니다. 다음에 개체 관리자를 사용할 수 있습니다.

- 네트워크, 포트, VLAN 또는 URL 개체를 사용하는 정책, 설정 및 기타 개체를 확인합니다. 자세한 내용은 개체 및 사용 현황 보기, 8 페이지의 내용을 참조하십시오.
- 여러 개체가 단일 설정을 참조하도록 개체를 그룹화하려면 개체 그룹, 10 페이지의 내용을 참조하십시오.
- 선택한 디바이스, 다중 도메인 구축, 선택된 도메인에서 개체 값을 오버라이드하려면 개체 재정의, 11 페이지의 내용을 참조하십시오.

액티브 정책에서 사용된 개체를 편집한 뒤 변경 설정을 재구축해야 변경 사항이 적용됩니다. 활성 정책에서 사용 되는 개체를 삭제할 수 없습니다.

참고 관리되는 디바이스에 할당된 정책에서 사용되는 경우에만 디바이스에 개체를 설정할 수 있습니다. 특정 디바이스에 할당된 모든 정책에서 개체를 제거하는 경우 개체는 다음 구축의 디바이스 설정에서 제거되고 개체에 대한 후속 변경 사항은 디바이스 설정에 반영되지 않습니다.

개체 유형

다음 표는 Firepower System에서 생성할 수 있는 개체 및 각 개체 유형이 그룹화 또는 오버라이드가 허용되는지 여부를 나타냅니다.

개체 유형	그룹화 가능?	오버라이드 허용?
네트워크	예	예
Port(포트)	예	예

개체 유형	그룹화 가능?	오버라이드 허용?
인터페이스: • 보안 영역 • 인터페이스 그룹	아니요	아니요
터널 영역	아니요	아니요
애플리케이션 필터	아니요	아니요
VLAN Tag	예	예
외부 속성: SGT(Security Group Tag) 및 동적 개체	아니요	아니요
URL	예	예
지리위치	아니요	아니요
시간 범위	아니요	아니요
변수 세트	아니요	아니요
Security Intelligence(보안 인텔리전스): 네트워크, DNS, URL 목록 및 피드	아니요	아니요
싱크홀	아니요	아니요
파일 목록	아니요	아니요
암호 그룹 목록	아니요	아니요
고유 이름	예	아니요
PKI(Public Key Infrastructure): • 내부 및 신뢰할 수 있는 CA • 내부 및 외부 인증	예	아니요
키 체인	아니요	예
DNS 서버 그룹	아니요	아니요
SLA 모니터링	아니요	아니요
접두사 목록: IPv4 및 IPv6	아니요	예
경로 맵	아니요	예
액세스 목록: 표준 및 확장	아니요	예

개체 유형	그룹화 가능**?**	오버라이드 허용**?**
AS 경로	아니요	예
커뮤니티 목록	아니요	예
정책 목록	아니요	예
FlexConfig: 텍스트 및 FlexConfig 개체	아니요	예

개체 및 멀티 테넌시

다중 도메인 구축에서 전역 도메인에서만 생성할 수 있는 SGT(보안 그룹 태그) 개체를 제외하고 전역 및 하위 도메인에 개체를 만들 수 있습니다. 시스템은 현재 도메인에 생성되어 편집할 수 있는 개체를 표시합니다. 또한 상위 도메인에 생성된 개체 중 보안 영역 및 인터페이스 그룹을 제외하고 편집이 불가능한 개체를 표시합니다.

참고 보안 영역 및 인터페이스 그룹은 리프 레벨에서 구성하는 디바이스 인터페이스와 연결되어 있으므로 하위 도메인의 관리자는 상위 도메인에 생성된 영역 및 그룹을 보고 편집할 수 있습니다. 서브도메인 사용자는 상위 영역 및 그룹에서 인터페이스를 추가하고 삭제할 수 있지만 영역/그룹을 삭제하거나 이름을 변경할 수 없습니다.

개체 이름은 도메인 계층 내에서 고유해야 합니다. 시스템은 현재 도메인에서 확인할 수 없는 개체 이름과의 충돌을 식별할 수 있습니다.

그룹화를 지원하는 개체의 경우 상위 도메인에서 상속된 개체를 포함해 현재 도메인에 있는 개체를 그룹화할 수 있습니다.

개체 오버라이드는 네트워크, 포트, VLAN 태그, URL 등 특정 유형의 개체에 대해 디바이스별 또는 도메인별 값을 정의하도록 합니다. 다중 도메인 구축에서 상위 도메인의 개체에 대한 기본값을 정의할 수 있지만 하위 도메인의 관리자가 해당 개체에 대한 오버라이드 값을 추가할 수 있습니다.

개체 관리자

개체 관리자를 사용해 개체 및 개체 그룹을 생성하고 관리할 수 있습니다.

개체 관리자는 페이지당 20개의 개체 또는 그룹을 표시합니다. 모든 유형의 개체 또는 그룹이 20개 이상 있는 경우, 추가 페이지를 보려면 페이지 하단의 탐색 링크를 사용합니다. 또한 특정 페이지로 이동하거나 **Refresh(**새로 고침**)(**)을 클릭하여 보기를 새로 고칠 수 있습니다.

기본적으로, 페이지는 개체 및 그룹을 이름의 알파벳 순으로 나열합니다. 페이지의 개체를 이름 또는 값으로 필터링할 수 있습니다.

개체 가져오기

쉼표로 구분된 값 파일에서 개체를 가져올 수 있습니다. 한 번에 최대 1,000개의 개체를 가져올 수 있습니다. 쉼표로 구분된 값 파일의 내용은 특정 형식을 따라야 합니다. 형식은 개체 유형마다 다릅니다. 몇 가지 유형의 개체만 가져올 수 있습니다. 지원되는 개체 유형 및 해당 규칙을 확인하려면 다음 표를 참조하십시오.

개체 유형	규칙

개별 개체	• 열 헤더는 대문자로 입력해야 합니다.
	• 파일에 다음 열 헤더가 있어야 합니다.
	  • 이름
	  • DN
	• 항목을 가져오려면 NAME 및 DN 열 항목이 모두 필요합니다.
	• 개별 개체를 기존의 고유 이름 개체 그룹으로 직접 가져올 수 있습니다.

네트워크 개체	• 열 헤더는 대문자로 입력해야 합니다.
	• 파일에 다음 열 헤더가 있어야 합니다.
	  • 이름
	  • 설명
	  • 유형
	  • 값
	  • 조회
	• 호스트, 범위 또는 네트워크 개체 유형의 항목을 가져오려면 NAME 및 VALUE 열 항목은 필수입니다.
	• FQDN 개체의 경우 TYPE 열 항목은 'fqdn'을 언급하고 LOOKUP 열 항목은 'ipv4,' 'ipv6,'또는 'ipv4_ipv6'으로 지정해야 합니다.
	• FQDN 개체의 LOOKUP 열 항목에 콘텐츠가 제공되지 않으면 개체는 ipv4_ipv6 필드 값과 함께 저장됩니다.

개체 유형	규칙

포트	• 열 헤더는 대문자로 입력해야 합니다.
	• 파일에 다음 열 헤더가 있어야 합니다.
	  • 이름
	  • PROTOCOL
	  • PORT
	  • ICMPCODE
	  • ICMPTYPE
	• NAME 열 항목은 필수입니다.
	• 'tcp' 및 'udp' 프로토콜 유형의 경우 PORT 열 항목은 필수입니다.
	• 'icmp' 및 'icmp6' 프로토콜 유형의 경우 ICMPCODE 및 ICMPTYPE 열 항목은 필수입니다.

URL	• 열 헤더는 대문자로 입력해야 합니다.
	• 파일에 다음 열 헤더가 있어야 합니다.
	  • 이름
	  • 설명
	  • URL
	• NAME 및 URL 열 항목은 필수 항목입니다.

VLAN Tag	• 열 헤더는 대문자로 입력해야 합니다.
	• 파일에 다음 열 헤더가 있어야 합니다.
	  • 이름
	  • 설명
	  • 태그
	• 항목을 가져오려면 NAME 및 TAG 열 항목은 필수입니다.

프로시저

단계 **1** **Objects(**개체**)** > **Object Management(**개체 관리**)**를 선택합니다.

단계 **2** 왼쪽 창에서 다음 개체 유형 중 하나를 선택합니다.

- **Distinguished Name(**고유 이름**)** > **Individual Objects(**개별 개체**)** >
- 네트워크 개체
- **Port(**포트**)**
- **URL**
- **VLAN Tag**

단계 **3** **Add [Object Type]([**개체 유형**]** 추가**)** 드롭다운 목록에서 **Import Object(**개체 가져오기**)**를 선택합니다.

참고 이전 단계에서 **Individual Objects(**개별 개체**)**를 선택한 경우 **Import(**가져오기**)**를 클릭합니다.

단계 **4** **Browse(**찾아보기**)**를 클릭합니다.

단계 **5** 시스템에서 쉼표로 구분된 파일을 찾아 선택합니다.

단계 **6** **Open(**열기**)**을 클릭합니다.

참고 **Distinguished Name(**고유 이름**)** 개체를 가져오는 동안 필요에 따라 **Add imported Distinguished Name objects to the below object group(**가져온 고유 이름 개체를 아래 개체 그룹에 추가 확인란을 선택하고 드롭 다운 상자에서 그룹 이름을 선택하여 개체를 기존의 고유 이름 개체 그룹으로 직접 가져올 수 있습니다.

단계 **7** **Import(**가져오기**)**를 클릭합니다.

개체 수정

다중 도메인 구축에서 시스템은 현재 도메인에서 생성된 개체를 표시하며 이러한 개체는 수정할 수 있습니다. 상위 도메인에서 생성된 개체도 표시되지만, 이러한 개체는 수정할 수 없습니다. 하위 도메인에서 생성된 개체를 보고 수정하려면 해당 도메인으로 전환하십시오.

프로시저

단계 **1** **Objects(**개체**)** > **Object Management(**개체 관리**)**을(를) 선택합니다.

단계 **2** 목록에서 개체 유형을 선택하려면 개체 소개, 2 페이지을 참조하십시오.

단계 **3** 편집하려는 개체 옆의 **Edit(**수정**)** ( )을 클릭합니다.

View(보기**)** ( )이 대신 표시되는 경우에는 개체가 상위 도메인에 속하며 재정의를 허용하지 않도록 설정되었거나 개체를 수정할 권한이 없는 것입니다.

단계 **4** 필요에 맞게 개체 설정을 수정합니다.

단계 **5** 변수 집합을 편집하는 경우 집합의 변수를 관리하려면 변수 관리, 108 페이지을 참조하십시오.

단계 **6** 오버라이드를 허용하도록 구성할 수 있는 개체는 다음과 같습니다.

- 이 개체에 대한 재정의를 허용하려면 **Allow Overrides(**재정의 허용**)** 확인란을 선택합니다. 개체 재정의 허용, 13 페이지의 내용을 참조하십시오. 현재 도메인에 속한 개체에 대해서만 이 설정을 변경할 수 있습니다.
- 이 개체에 재정의 값을 추가하려면 Override(재정의) 섹션을 펼치고 **Add(**추가**)**를 클릭합니다. 개체 재정의 추가, 14 페이지의 내용을 참조하십시오.

단계 **7** **Save(**저장**)**를 클릭합니다.

단계 **8** 변수 집합을 편집하고 해당 집합이 액세스 제어 정책에서 사용 중인 경우 변경 사항을 저장하려면 **Yes(**예**)**를 클릭합니다.

다음에 수행할 작업

- 활성 정책이 개체를 참조하는 경우 구성 변경 사항을 구축합니다. 참조.

개체 및 사용 현황 보기

Object Management(개체 관리) 페이지에서 개체의 사용량 세부 정보를 볼 수 있습니다. Management Center에서는 많은 개체 유형에 대해 이 기능을 제공합니다. 그러나 일부 개체 유형은 지원되지 않습니다.

참고 다중 도메인 구축에서는 다른 도메인의 개체를 확인할 수 있습니다. 하지만 하위 도메인의 개체 사용량을 확인하려면 해당 도메인으로 전환해야 합니다.

프로시저

단계 **1** **Objects(**개체**)** > **Object Management(**개체 관리**)**를 선택합니다.

단계 **2** 지원되는 다음 개체 유형 중 하나를 선택합니다.

- 액세스 목록 > 확장
- 액세스 목록 > 표준
- AS 경로
- 커뮤니티 목록
- 인터페이스
- 네트워크
- 정책 목록

- 포트
- 접두사 목록> IPv4 접두사 목록
- 접두사 목록> IPv6 접두사 목록
- 경로 맵
- SLA 모니터링
- URL
- VLAN Tag

단계 **3** 개체 옆에 있는 **Find Usage(**사용량 찾기**)(**) 아이콘을 클릭합니다.

Object Usage(개체 사용량) 창에는 개체가 사용 중인 모든 정책, 개체 및 기타 설정 목록이 표시됩니다. 목록에 있는 항목을 클릭하면 개체 사용량 추가 정보를 확인할 수 있습니다. 개체를 사용하는 정책 및 일부 기타 설정의 경우, 해당 링크를 클릭하면 대응하는 UI 페이지를 방문할 수 있습니다.

개체 또는 개체 그룹 필터링

다중 도메인 구축에서 시스템은 필터링 가능한 현재 및 상위 도메인에서 생성된 개체를 표시합니다.

프로시저

단계 **1** **Objects(**개체**)** > **Object Management(**개체 관리**)**을(를) 선택합니다.

단계 **2** **Filter(**필터**)** 필드에 필터 기준을 입력합니다.

일치하는 항목을 입력하여 표시하면 페이지가 업데이트됩니다.

다음 와일드카드를 사용할 수 있습니다.

- 별표(*)는 0번 이상 나타나는 문자에 해당합니다.
- 캐럿 (^) 은 문자열의 시작 부분에 있는 내용에 해당합니다.
- 달러 기호 ($)는 문자열의 끝 부분에 있는 내용에 해당합니다.

단계 **3** 시스템에서 사용되지 않는 개체 및 개체 그룹을 보려면 **Show Unused Object(**사용하지 않은 개체 표시**)** 확인란을 선택합니다.

참고

- 개체가 사용되지 않은 개체 그룹의 일부인 경우, 개체는 사용된 것으로 간주됩니다. 그러나 **Show Unused Object(**사용되지 않은 개체 표시**)** 확인란을 선택하면 사용되지 않은 개체 그룹이 표시됩니다.
- **Show Unused Object(**사용되지 않은 개체 표시**)** 확인란은 네트워크, 포트, URL 및 VLAN 태그 개체 유형에만 사용할 수 있습니다.

개체 그룹

개체 그룹화는 단일 컨피그레이션으로 여러 개체를 참조하도록 허용합니다. 시스템을 통해 웹 인터페이스에서 개체 및 개체 그룹을 같은 의미로 사용할 수 있습니다. 예를 들어, 포트 개체를 사용하는 모든 곳에서 포트 개체 그룹을 사용할 수 있습니다.

네트워크, 포트, VLAN 태그, URL, PKI 개체를 그룹화할 수 있습니다. 네트워크 개체 그룹은 중첩될 수 있습니다. 즉 네트워크 개체 그룹을 최대 10레벨까지 다른 네트워크 개체 그룹에 추가할 수 있습니다.

유형이 동일한 개체 및 개체 그룹이 동일한 이름을 가질 수 없습니다. 다중 도메인 구축에서 개체 그룹 이름은 도메인 계층 내에서 고유해야 합니다. 시스템은 현재 도메인에서 확인할 수 없는 개체 그룹 이름과의 충돌을 식별합니다.

정책에서 사용되는 개체 그룹(액세스 제어 정책의 네트워크 개체 그룹 등)을 편집할 때는 변경 설정을 재구축해야 변경 사항이 적용됩니다.

그룹을 삭제해도 그룹 내 개체는 삭제되지 않으며, 개체 간 연결만 삭제됩니다. 또한 활성 정책에서 사용 중인 그룹을 삭제할 수 없습니다. 예를 들어 저장한 액세스 제어 정책의 VLAN 조건에서 사용 중인 VLAN 태그 그룹은 삭제할 수 없습니다.

재사용 가능 개체 그룹화

다중 도메인 구축에서 시스템은 현재 도메인에서 생성된 개체를 표시하며 이러한 개체는 수정할 수 있습니다. 상위 도메인에서 생성된 개체도 표시되지만, 이러한 개체는 수정할 수 없습니다. 하위 도메인에서 생성된 개체를 보고 수정하려면 해당 도메인으로 전환하십시오.

상위 도메인에서 상속된 개체를 포함해 현재 도메인의 개체를 그룹화할 수 있습니다.

프로시저

단계 **1** **Objects(**개체**)** > **Object Management(**개체 관리**)**을(를) 선택합니다.

단계 **2** 그룹화할 개체 유형이 네트워크, 포트, **URL**, **VLAN** 태그인 경우:

a) 개체 유형 목록에서 개체 유형을 선택합니다.

b) 드롭다운 목록의 **Add [Object Type]([**개체 유형**]** 추가**)**에서 **Add Group(**그룹 추가**)**를 선택합니다.

단계 **3** 그룹화하려는 개체 유형이 **Distinguished Name(**고유 이름**)**인 경우:

a) **Distinguished Name(**고유 이름**)** 노드를 확장합니다.

b) **Object Group(**개체 그룹**)**을 선택합니다.
c) **Add Distinguished Name Group(**고유 이름 그룹 추가**)**을 클릭합니다.

단계 **4** 그룹화하려는 개체 유형이 **PKI**인 경우:

a) **PKI** 노드를 확장합니다.
b) 다음 중 하나를 선택합니다.

- 내부 **CA** 그룹
- 신뢰하는 **CA** 그룹
- 내부 인증서 그룹
- 외부 인증서 그룹

c) **Add [Object Type] Group([**개체 유형**]** 그룹 추가**)**을 클릭합니다.

단계 **5** 고유한 이름을 입력합니다.

단계 **6** 목록에서 하나 이상의 개체를 선택하고 **Add(**추가**)**를 클릭합니다.

다음 작업도 가능합니다.

- 기존 개체를 포함하여 검색하려면 필터 필드 **Search(**검색**)** ( )를 사용합니다. 입력 시 일치하는 항목이 업데이트됩니다. 검색 필드 위의 **Reload(**다시 로드**)**( )을 클릭하거나 검색 필드에서 **Clear(**지우기**)** ( )을 클릭하여 검색 문자열을 삭제합니다.
- 어떤 기존 개체도 요구 사항을 충족하지 않는 경우 **Add(**추가**)** ( )을 클릭하여 상황에 따라 개체를 생성합니다.

단계 **7** 네트워크, 포트, **URL**, **VLAN** 태그 그룹일 경우:

- **Description(**설명**)**을 입력합니다.
- 개체 그룹의 오버라이드를 허용하려면 체크 박스에서 **Allow Overrides(**오버라이드 허용**)**을 선택합니다. 개체 재정의 허용, 13 페이지를 참조하십시오.

단계 **8** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

- 활성 정책이 개체 그룹을 참조하는 경우 설정 변경을 구축하는 방법은 구성 변경 사항 구축을 참조하십시오.

개체 재정의

개체 오버라이드는 시스템이 지정한 장치에 대해 사용하는 개체에 대한 대체 값을 정의하도록 합니다.

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

예를 들어 다른 네트워크에 연결된 회사 내 다른 부서의 ICMP 트래픽을 거부하는 경우가 있습니다. 이런 경우 부서 네트워크라는 네트워크 개체가 포함된 규칙이 있는 액세스 제어 정책을 정의합니다. 이 개체에 대한 오버라이드를 허용함으로써 디바이스가 연결된 실제 네트워크를 지정하는 각 관련 디바이스의 오버라이드를 생성할 수 있습니다.

다중 도메인 구축에서 상위 도메인의 개체에 대한 기본값을 정의할 수 있지만 하위 도메인의 관리자가 해당 개체에 대한 오버라이드 값을 추가할 수 있습니다. 예를 들어 관리되는 보안 서비스 제공자(MSSP)는 여러 고객에 대한 네트워크 보안을 관리하기 위해 단일 management center를 사용할 수 있습니다. MSSP의 관리자는 모든 고객의 배포에 사용하기 위한 전역 도메인의 개체를 정의할 수 있습니다. 각 고객의 관리자는 조직에 대한 개체를 오버라이드하기 위해 하위 도메인에 로그인할 수 있습니다. 이런 로컬 관리자는 MSSP 내 다른 고객의 오버라이드 값을 보거나 영향을 줄 수 없습니다.

특정 도메인에 개체 오버라이드를 지정할 수 없습니다. 이 경우 시스템은 사용자가 디바이스 수준에서 오버라이드하지 않는 경우 대상 도메인의 모든 디바이스에 개체 오버라이드 값을 사용합니다.

개체 관리자에서 오버라이드 가능한 개체를 선택하고 개체에 대해 디바이스 수준 또는 도메인 수준의 오버라이드 목록을 정의할 수 있습니다.

다음 개체 유형에만 개체 오버라이드를 사용할 수 있습니다.

- 네트워크
- Port(포트)
- VLAN 태그
- URL
- SLA 모니터링
- 접두사 목록
- 경로 맵
- 액세스 목록
- AS 경로
- 커뮤니티 목록
- 정책 목록
- PKI 등록
- 키 체인

개체를 오버라이드할 수 있는 경우 개체 관리자의 개체 유형에 **Override(**재정의**)** 열이 나타납니다. 이 열에서 사용 가능한 값은 다음과 같습니다.

- 녹색 확인 표시 - 개체에 대한 오버라이드를 만들 수 있으며 오버라이드가 추가된 적이 없음을 나타냅니다.
- 빨간색 X - 해당 개체에는 오버라이드를 생성할 수 없음을 나타냅니다.
- 숫자 - 해당 개체에 추가된 오버라이드의 수를 나타냅니다. (예를 들어 "2"는 2개의 오버라이드가 추가됐음을 나타냅니다.)

개체 재정의 관리

프로시저

단계 **1** **Objects(**개체**)** > **Object Management(**개체 관리**)**을(를) 선택합니다.

단계 **2** 개체 유형 목록에서 선택합니다. 개체 소개, 2 페이지을 참조하십시오.

단계 **3** 편집하려는 개체 옆의 **Edit(**수정**)** ( )을 클릭합니다.

View(보기**)** ( )이 대신 표시되는 경우에는 개체가 상위 도메인에 속하며 재정의를 허용하지 않도록 설정되었거나 개체를 수정할 권한이 없는 것입니다.

단계 **4** 개체 오버라이드 관리

- 추가 - 개체 오버라이드를 추가합니다. 개체 재정의 추가, 14 페이지을 참조하십시오.
- 허용 - 개체 오버라이드를 허용합니다. 개체 재정의 허용, 13 페이지을 참조하십시오.
- 삭제 - 개체 편집기에서 제거하려는 오버라이드 옆의 **Delete(**삭제**)** ( )를 클릭합니다.
- 편집 - 오버라이드를 편집합니다. 개체 오버라이드 편집, 14 페이지을 참조하십시오.

개체 재정의 허용

프로시저

단계 **1** 개체 편집기에서 **Allow Overrides(**재정의 허용**)** 확인란을 선택합니다.

단계 **2** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

개체 재정의 값을 추가합니다. 개체 재정의 추가, 14 페이지를 참조하십시오.

개체 재정의 추가

시작하기 전에

개체 재정의를 허용합니다. 개체 재정의 허용, 13 페이지를 참조하십시오.

프로시저

단계 **1** 개체 편집기에서 **Override(**재정의**)** 섹션을 확장합니다.

단계 **2** **Add(**추가**)**를 클릭합니다.

단계 **3** **Targets(**타겟**)**에서 **Available Devices and Domains(**사용 가능한 디바이스 및 도메인**)** 목록에서 도메인 또는 디바이스를 선택하고 **Add(**추가**)**를 클릭합니다.

단계 **4** Override(재정의) 탭에서 **Name(**이름**)**을 입력합니다.

단계 **5** 필요한 경우 **Description(**설명**)**을 입력합니다.

단계 **6** 재정의 값을 입력합니다.

예제**:**

네트워크 개체의 경우 네트워크 값을 입력합니다.

단계 **7** **Add(**추가**)**를 클릭합니다.

단계 **8** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

- 활성 정책이 개체를 참조하는 경우 구성 변경 사항을 구축합니다. 참조.

개체 오버라이드 편집

기존 오버라이드 값과 설명은 수정할 수 있지만 기존 대상 목록은 수정할 수 없습니다. 대신 기존 오버라이드를 대체하는 새 대상에 새 오버라이드를 추가해야합니다.

프로시저

단계 **1** 개체 편집기에서 **Override(**재정의**)** 섹션을 확장합니다.

단계 **2** 수정할 오버라이드 옆의 **Edit(**수정**)** ( )을 클릭합니다.

단계 **3** 필요에 따라 설명을 수정합니다.

단계 **4** 오버라이드 값을 수정합니다.

단계 **5** **Save(**저장**)**를 클릭하여 오버라이드를 저장합니다.

단계 **6** **Save(**저장**)**를 클릭하여 개체를 저장합니다.

다음에 수행할 작업

- 활성 정책이 개체를 참조하는 경우 구성 변경 사항을 구축합니다. 참조.

AAA 서버

재개 가능한 AAA 서버 개체를 추가합니다.

RADIUS 서버 그룹 추가

RADIUS 서버 그룹 개체는 RADIUS 서버에 대한 하나 이상의 참조를 포함합니다. 이러한 서버는 원격 액세스 VPN 연결을 통해 로그인하는 사용자를 인증하는 데 사용됩니다.

이 개체는 threat defense 디바이스와 함께 사용할 수 있습니다.

시작하기 전에

참고 RADIUS 서버 그룹 개체는 오버라이드할 수 없습니다.

프로시저

단계 **1** **Object(**개체**)** > **Object Management(**개체 관리**)** > **AAA Server(AAA** 서버**)** > **RADIUS Server Group(RADIUS** 서버 그룹**)**을 선택합니다.

현재 구성된 모든 RADIUS 서버 그룹 개체가 나열됩니다. 필터를 사용하여 목록을 축소합니다.

단계 **2** 나열된 RADIUS 서버 그룹 개체를 선택하고 편집하거나 새로 추가합니다.

이 개체를 구성할 땐 RADIUS 서버 옵션, 17 페이지과 RADIUS 서버 그룹 옵션, 15 페이지를 참조하십시오.

단계 **3** **Save(**저장**)**를 클릭합니다.

RADIUS 서버 그룹 옵션

탐색 경로

Objects(개체**)** > **Object Management(**개체 관리**)** > **AAA Server(AAA** 서버**)** > **RADIUS Server Group(RADIUS** 서버 그룹**)**. 구성된 RADIUS 서버 그룹 개체를 선택하고 편집하거나 새로 추가합니다.

필드

- 이름 및 설명 - 이름을 입력하고 필요에 따라 RADIUS 서버 그룹 개체를 식별할 설명을 입력합니다.
- 그룹 계정 모드 - 그룹의 RADIUS 서버에 어카운팅 메시지를 전송하는 방법입니다. 단일을 선택하면 어카운팅 메시지가 그룹의 단일 서버에 전송됩니다. 기본 설정입니다. **Multiple(**다중**)**을 선택하면 그룹 내 모든 서버에 동시에 어카운팅 메시지가 전송됩니다.
- 재시도 간격 - RADIUS 서버에 연결을 시도하는 간격입니다. 값의 범위는 1~10초입니다.
- 영역(선택 사항) - 이 RADIUS 서버 그룹이 연결될 Active Directory(AD) 영역을 지정 또는 선택합니다. 영역은 트래픽 플로우에 대한 VPN 인증 ID 소스를 결정하는 경우 연결된 RADIUS 서버 그룹에 액세스하기 위해 ID 정책에서 선택됩니다. 이 영역은 ID 정책에서 RADIUS 서버 그룹을 연결하는 브리지를 효과적으로 제공합니다. RADIUS 서버 그룹에 어떤 영역도 연결되지 않은 경우, ID 정책의 트래픽 플로우에 대한 VPN 인증 ID 소스를 결정할 때 RADIUS 서버 그룹을 연결할 수 없습니다.

참고 사용자 ID 및 RADIUS를 ID 소스로 사용하는 원격 액세스 VPN을 사용하는 경우 이 필드는 필수입니다.

- 권한 부여 전용 모드 활성화 - 이 RADIUS 서버 그룹이 인증에 사용되지 않지만 권한 부여 또는 계정 관리에 사용되는 경우 이 필드를 활성화하여 RADIUS 서버 그룹에 권한 부여 전용 모드를 활성화합니다.

  권한 부여 전용 모드는 Access-Request에서 RADIUS 서버 비밀번호를 포함해야 할 필요가 없습니다. 따라서 개별 RADIUS 서버에 대해 구성된 비밀번호는 무시됩니다.
- 중간 계정 업데이트 활성화 및 간격 - 새로 할당된 IP 주소의 RADIUS 서버를 알려주기 위해 RADIUS 중간 계정 관리 업데이트 메시지를 생성할 수 있습니다. 간격 필드의 주기적인 계정 관리 업데이트 간 시간 간격을 시간 단위로 설정합니다. 유효한 범위는 1에서 120이며 기본값은 24입니다.
- 동적 권한 부여 활성화 및 포트 - RADIUS 서버 그룹에 대한 RADIUS 동적 권한 부여 또는 CoA(Change of Authorization) 서비스를 활성화합니다. 포트 필드에서 RADIUS CoA 요청에 대한 수신 대기 포트를 지정합니다. 기본값은 1700이고, 범위는 1024~65535입니다. 일단 정의되면 해당 RADIUS 서버 그룹이 CoA 알림에 등록되고 ISE(Cisco Identity Services Engine)에서 보내는 CoA 정책 업데이트를 포트에서 수신합니다.
- **RADIUS** 서버 - RADIUS 서버 옵션, 17 페이지를 참조합니다.

관련 항목

RADIUS 서버 그룹 추가, 15 페이지

RADIUS 서버 옵션

탐색 경로

Object(개체**)** > **Object Management(**개체 관리**)** > **AAA Server(AAA** 서버**)** > **RADIUS Server Group(RADIUS** 서버 그룹**)**. 나열된 RADIUS 서버 그룹 개체를 선택하고 편집하거나 새로 추가합니다. 이후 RADIUS 서버 그룹 대화 상자에서 나열된 RADIUS 서버를 선택하고 수정하거나 새로 추가합니다.

필드

- **IP** 주소/호스트 이름 - 인증 요청이 전송되는 RADIUS 서버의 호스트 이름 또는 IP 주소를 식별하는 네트워크 개체입니다. RADIUS 서버 그룹 목록에 추가 RADIUS 서버 또는 추가 서버를 추가하려면 하나만 선택할 수 있습니다.

참고 디바이스는 이제 RADIUS 인증에 IPv6 IP 주소를 지원합니다.

- **Authentication Port(**인증 포트**)** - RADIUS 인증 및 권한 부여가 수행되는 포트입니다. 기본값은 1,812입니다.
- 키 및 키 확인 - 매니지드 디바이스(클라이언트) 및 RADIUS 서버 간 데이터를 암호화하는 데 사용되는 공유 암호입니다.

  키는 대소문자를 구분하며 최대 127자의 영숫자입니다. 특수 문자가 허용됩니다.

  이 필드에 정의된 키는 RADIUS 서버 키와 일치해야 합니다. 확인 필드에 키를 다시 입력합니다.
- 어카운팅 포트 - RADIUS 어카운팅을 수행하는 포트입니다. 기본값은 1,813입니다.
- 시간 초과 - 인증에 대한 세션 시간 초과입니다.

참고 RADIUS의 두 인증 요소에 대한 시간 초과 값은 60초 이상이어야 합니다. 기본 시간 제한 값은 10초입니다.

- 연결 사용 - 경로 조회 또는 특정 이터페이스를 사용해 디바이스에서 RADIUS 서버로의 연결성을 설정합니다.
  - 라우팅 테이블을 사용하려면 **Routing(**라우팅**)** 라디오 버튼을 클릭합니다.
  - **Specific Interface(**특정 인터페이스**)** 라디오 버튼을 클릭하고 드롭다운 목록에서 보안 영역/인터페이스 그룹 또는 진단 인터페이스(기본값)를 선택합니다.
- 재전송 **ACL** - 목록에서 재전송 ACL을 선택하거나 새 ACL을 추가합니다.

참고 재전송될 트래픽을 결정하는 디바이스에서 정의된 ACL의 이름입니다. 이 재전송 ACL 이름은 ISE 서버의 재전송 *ACL*과 동일해야 합니다. ACL 개체를 구성하는 경우 ISE 및 DNS 서버에 차단 작업을 선택하거나 나머지 서버에 허용 작업을 선택합니다.

관련 항목

RADIUS 서버 그룹 추가, 15 페이지
RADIUS 서버 그룹 옵션, 15 페이지

SSO(Single Sign-On) 서버 추가

시작하기 전에

SAML ID 공급자에서 다음 정보를 가져옵니다.

- ID 제공자 엔티티 ID URL
- 로그인 URL
- 로그아웃 URL
- ID 제공자 인증서 및 management center 웹 인터페이스를 사용하여 threat defense에 인증서 등록 (**Devices (**디바이스**)** > **Certificates (**인증서**)**)

자세한 내용은 SAML SSO(Single Sign-On) 인증 구성를 참고하십시오.

프로시저

단계 **1** **Object(**개체**)** > **Object Management(**개체 관리**)** > **AAA Server(AAA** 서버**)** > **Single Sign-on Server(SSO(Single Sign-On)** 서버**)**를 선택합니다.

단계 **2** **Add Single Sign-on Server(SSO(Single Sign-On)** 서버 추가**)**를 클릭하고 다음 세부 정보를 제공합니다.

- **Name(**이름**)** - SAML SSO 서버 개체의 이름입니다.
- **Identity Provider Entity ID(ID** 공급자 엔터티 **ID)** - 서비스 공급자를 고유하게 식별하기 위해 SAML IdP에 정의된 URL입니다.

  SAML 발급자가 요청에 응답하는 방법을 설명하는 메타데이터 XML을 제공하는 페이지의 URL입니다.
- **SSO URL** — ID 공급자 서버에 로그인하기 위한 URL입니다.
- **Logout URL(**로그아웃 **URL)** - ID 공급자 서버에서 로그아웃하기 위한 URL입니다.

- **Base URL(**기본 **URL)** - ID 공급자 인증이 완료되면 사용자를 threat defense로 다시 리디렉션하는 URL입니다. threat defense 원격 액세스 VPN용으로 설정된 액세스 인터페이스의 URL입니다.
- **Identity Provider Certificate(ID** 공급자 인증서**)** - IdP에서 서명한 메시지를 확인하기 위해 threat defense에 등록된 IdP의 인증서입니다.

  목록에서 식별 제공자 인증서를 선택하거나 Add(추가)를 클릭하여 새 인증서 등록 개체를 생성합니다.

  자세한 내용은 Threat Defense 인증서 매핑를 참고하십시오.

  모든 Microsoft Azure 등록 애플리케이션 CA 인증서를 threat defense의 신뢰 지점으로 등록해야 합니다. Microsoft Azure SAML ID 제공자가 초기 애플리케이션에 대해 threat defense에 구성됩니다. 모든 연결 프로파일은 구성된 MS Azure SAML ID 제공자에 매핑됩니다. 각 MS Azure 애플리케이션(기본값 제외)에 대해 원격 액세스 VPN의 연결 프로파일 구성에서 필요한 트러스트 포인트(CA 인증서)를 선택할 수 있습니다.

  자세한 내용은 Remote Access VPN에 대한 AAA 설정를 참조하십시오.
- **Service Provider Certificate(**서비스 공급자 인증서**)** - 요청에 서명하고 IdP와의 신뢰 관계를 구축하는 데 사용되는 threat defense 인증서입니다.

  내부 threat defense 인증서를 등록하지 않은 경우 +를 클릭하여 인증서를 추가하고 등록합니다. 자세한 내용은 Threat Defense 인증서 매핑를 참고하십시오.
- **Request Signature(**요청 서명**)** - SAML SSO(Single Sign-On) 요청에 서명할 암호화 알고리즘을 선택합니다.

  서명은 SHA1, SHA256, SHA384, SHA512와 같이 가장 약한 항목부터 가장 강력한 항목까지 나열됩니다. 암호화를 비활성화하려면 None(없음)을 선택합니다.
- **Request Timeout(**요청 시간 초과**)** - 사용자가 단일 SSO 요청을 완료하는 데 사용할 SAML 어설션 유효 기간을 지정합니다. SAML IdP에는 *NotBefore* 및 *NotOnOrAfter*의 두 가지 시간 초과가 있습니다. threat defense는 현재 시간이 (하한) *NotBefore* 및 (상한) 시간 범위 내에 있는지 확인하고 *NotBefore* + 시간 초과 및 *NotOnOrAfter* 중 작은 시간 범위 내에 있는지 확인합니다. 따라서 시간 초과를 IdP의 *NotOnOrAfter* 시간 초과보다 길게 설정하면 지정된 시간 초과가 무시되고 *NotOnOrAfter* 시간 초과가 선택됩니다. 지정된 시간 초과와 *NotBefore* 시간 초과의 합계가 *NotOnOrAfter* 시간보다 작으면 threat defense 시간 초과가 시간 초과를 재정의합니다.

  시간 초과 범위는 1-7200초이며, 기본 시간 초과는 300초입니다.
- **Enable IdP only access on Internal Network(**내부 네트워크에서만 액세스 가능한 **IdP** 활성화**)** - SAML IdP가 내부 네트워크에 상주하는 경우 이 옵션을 선택합니다. Threat Defense는 게이트웨이 역할을 하며 익명 webvpn 세션을 사용하여 사용자와 IdP 간의 통신을 설정합니다.
- **Request IdP re-authentication on Login(**로그인 시 **IdP** 재인증 요청**)** - 이전 IdP 세션이 유효한 경우에도 각 로그인 시 사용자를 인증하려면 이 옵션을 선택합니다.
- **Allow Overrides(**재정의 허용**)** - 이 SSO 서버 개체에 대한 재정의를 허용하려면 이 체크 박스를 선택합니다.

단계 **3** **Save(**저장**)**를 클릭합니다.

관련 항목

Remote Access VPN에 대한 AAA 설정

액세스 목록

ACL(Access Control List)이라고도 알려진 액세스 목록 개체는 서비스를 적용할 트래픽을 선택합니다. threat defense 디바이스에 대해 경로 맵과 같은 특별한 기능을 설정할 때 이러한 개체를 사용합니다. ACL에 의해 허용으로 식별된 트래픽은 서비스가 제공되는 반면 "차단된" 트래픽은 서비스에서 제외됩니다. 서비스에서 제외된 트래픽은 반드시 삭제된다는 의미는 아닙니다.

다음 유형의 ACL을 구성할 수 있습니다.

- 확장 - 소스 및 대상 주소와 포트를 기반으로한 트래픽을 식별합니다. 특정 규칙을 혼합할 수 있는 IPv4 및 IPv6 주소를 지원합니다.
- 표준 - 대상 주소만을 기반으로 트래픽을 식별합니다. IPv4만 지원합니다.

ACL은 하나 이상의 ACE(액세스 제어 항목) 또는 규칙으로 구성됩니다. ACE의 순서는 중요합니다. 패킷이 "허용된" ACE와 일치하는지 평가하는 데 ACL이 사용되면, 패킷은 각 ACE 항목에 대해 항목이 나열된 순서에 따라 점검됩니다. 일치가 발견되면 ACE가 더 이상 점검되지 않습니다. 예를 들어 10.100.10.1을 "허용"하지만 10.100.10.0/24의 나머지는 "차단"하려는 경우 허용 항목은 차단 항목 앞에 위치해야 합니다. 일반적으로 더 구체적인 규칙이 ACL의 상단에 배치됩니다.

"허용" 항목과 일치하지 않는 패킷은 차단해야 할 패킷으로 간주됩니다.

다음 주제는 ACL 개체를 구성하는 방법을 설명합니다.

확장 **ACL** 개체 설정

소스, 대상 주소, 프로토콜, 포트 애플케이션 그룹을 기반으로 트래픽을 일치시키려고 하거나 트래픽이 IPv6인 경우 확장 ACL 개체를 사용합니다.

프로시저

단계 **1** 개체 > 개체 관리를 선택하고 목차에서 액세스 제어 목록 > 확장을 선택합니다.

단계 **2** 다음 중 하나를 수행합니다.

- 새 개체를 생성하려면 **Add Extended ACL(**확장 **ACL** 추가**)**를 클릭합니다.
- **Edit(**수정**)** ( )을 클릭하여 기존 개체를 편집합니다.

단계 **3** 확장 ACL 개체 대화 상자에서 개체의 이름을 입력(공백은 허용되지 않음)하고 액세스 제어 항목을 구성합니다.

a) 다음 중 하나를 수행합니다.

- **Add(**추가**)**를 클릭하여 새 엔트리를 만듭니다.
- **Edit(**수정**)** ( )을 클릭해서 기존 항목을 편집합니다.

마우스 오른쪽 버튼 클릭 메뉴에는 항목 잘라내기, 복사, 붙여넣기, 삭제 옵션이 포함되어 있습니다.

b) 작업을 선택하여 트래픽 조건을 허용(일치) 또는 차단(불일치)합니다.

참고 로그인, 로그 레벨, 로그 간격 옵션은 액세스 규칙에만 사용됩니다. (인터페이스에 속한 ACL 또는 전역으로 적용된 ACL) 액세스 규칙에 ACL 개체가 사용되지 않으므로 이 값을 기본값으로 유지합니다.

c) 다음 방법 중 하나를 사용하여 네트워크 탭에서 소스 및 대상 주소를 구성합니다.

- 사용 가능한 목록에서 원하는 네트워크 개체 또는 그룹을 선택하고 **Add to Source(**소스에 추가**)** 또는 **Add to Destination(**대상에 추가**)**를 클릭합니다. 목록 위의 +를 클릭하여 새 개체를 생성할 수 있습니다. IPv4 및 IPv6 주소를 혼합할 수 있습니다.
- 소스 또는 대상 목록 아래의 편집 상자에 주소를 입력하고 **Add(**추가**)**를 클릭합니다. 단일 호스트 주소(10.100.10.5 또는 2001:DB8::0DB8:800:200C:417A 등)나 서브넷(10.100.10.0/24 또는 10.100.10.0 255.255.255.0 형식, 또는 IPv6의 경우 2001:DB8:0:CD30::/60)를 지정할 수 있습니다.

d) 포트 탭을 클릭하고 다음 방법 중 하나를 사용하여 서비스를 구성합니다.

- 사용 가능한 목록에서 원하는 포트 개체를 선택하고 **Add to Source(**소스에 추가**)** 또는 **Add to Destination(**대상에 추가**)**를 클릭합니다. 목록 위의 +를 클릭하여 새 개체를 생성할 수 있습니다. 개체는 TCP/UDP 포트, ICMP/ICMPv6 메시지 유형, ("any" 포함) 다른 프로토콜을 지정할 수 있습니다. 그러나 일반적으로 비워 두는 소스 포트는 TCP/UDP만 수락합니다. 포트 그룹은 선택할 수 없습니다.

  TCP/UDP의 경우 둘 다 지정하는 경우 소스 및 대상 필드에서 동일한 프로토콜을 사용해야 합니다. 예를 들어 UDP 소스 포트 및 TCP 대상 포트를 지정할 수 없습니다.
- 소스 또는 대상 목록 아래의 편집 상자에 포트 또는 프로토콜을 입력하거나 선택하고 **Add(**추가**)**를 클릭합니다.

참고 모든 IP 트래픽에 적용되는 항목을 얻기 위해 "all(모든)" 프로토콜을 지정하는 대상 포트 개체를 선택합니다.

e) **Application(**애플리케이션**)** 탭을 클릭하고 직접 인터넷 액세스 정책에 대해 그룹화할 애플리케이션을 선택합니다.

중요
- 클러스터 디바이스에 대한 애플리케이션을 구성할 수 없습니다. 따라서 이 탭은 클러스터 디바이스에 적용되지 않습니다.
- 정책 기반 라우팅의 애플리케이션에만 확장 ACL을 사용합니다. 해당 동작을 알 수 없으며 지원되지 않으므로 다른 정책에서 사용하지 마십시오.

참고

- **Available Applications(**사용 가능한 애플리케이션**)** 목록에는 사전 정의된 고정된 애플리케이션 집합이 표시됩니다. 이 목록은 첫 번째 패킷(IP 주소 및 포트로 확인된 FQDN 엔드포인트)에 의해서만 탐지될 수 있으므로 액세스 제어 정책에서 사용 가능한 애플리케이션의 하위 집합입니다. 애플리케이션 정의는 VDB 업데이트를 통해 업데이트되며 후속 구축 중에 threat defense에 푸시됩니다.
- 사용자 정의 맞춤형 애플리케이션 또는 애플리케이션 그룹은 지원되지 않습니다.
- 현재 management center는 사용자 정의 맞춤형 애플리케이션 또는 애플리케이션 그룹을 지원하지 않으며 사전 정의된 애플리케이션 목록을 수정할 수 없습니다.
- **Application Filters(**애플리케이션 필터**)** 아래에 제공된 필터 옵션을 사용하여 이 목록을 구체화할 수 있습니다.

f) 필요한 애플리케이션을 선택하고 **Add to Rule(**규칙에 추가**)**을 클릭합니다.

참고

- 확장 ACL 개체에서 대상 네트워크 및 애플리케이션을 구성하지 마십시오.
- 각 액세스 제어 항목에서 선택한 애플리케이션(Nertwork 서비스 개체)은 NSG(네트워크 서비스 그룹)를 형성하며 이 그룹은 threat defense에 구축됩니다. NSG는 직접 인터넷 액세스에서 선택한 애플리케이션 그룹과의 일치를 기준으로 트래픽을 분류하는 데 사용됩니다.

g) 개체에 해당 항목을 추가하려면 **Add(**추가**)**를 클릭합니다.

h) 필요한 경우 항목을 클릭한 뒤 위나 아래로 드래그하여 규칙 순서에서 원하는 위치로 이동합니다.

개체에 추가 항목을 생성하거나 편집하려면 프로세스를 반복합니다.

단계 **4** 이 개체에 대한 재정의를 허용하려면 **Allow Overrides(**재정의 허용**)** 확인란을 선택합니다. 개체 재정의 허용, 13 페이지의 내용을 참조하십시오.

단계 **5** **Save(**저장**)**를 클릭합니다.

표준 **ACL** 개체 설정

대상 IPv4 주소만에 기반해 트래픽을 일치시키려면 표준 ACL 개체를 사용합니다. 그 외에는 확장 ACL을 사용합니다.

프로시저

단계 **1** 개체 > 개체 관리를 선택하고 목차에서 액세스 제어 목록 > 표준을 선택합니다.

단계 **2** 다음 중 하나를 수행합니다.

- 새 개체를 생성하려면 **Add Standard ACL(**표준 **ACL** 추가**)**를 클릭합니다.

- **Edit(**수정**)** ( )을 클릭하여 기존 개체를 편집합니다.

단계 **3** 표준 ACL 개체 대화 상자에서 개체의 이름을 입력(공백은 허용되지 않음)하고 액세스 제어 항목을 구성합니다.

a) 다음 중 하나를 수행합니다.

- **Add(**추가**)**를 클릭하여 새 엔트리를 만듭니다.
- **Edit(**수정**)** ( )을 클릭해서 기존 항목을 편집합니다.

마우스 오른쪽 버튼 클릭 메뉴에는 항목 잘라내기, 복사, 붙여넣기, 삭제 옵션이 포함되어 있습니다.

b) 각 액세스 제어 항목에 대해 다음 속성을 구성합니다.

- 작업 - 트래픽 조건을 허용(일치) 또는 차단(불일치)합니다.
- 네트워크 - IPv4 네트워크 개체 또는 트래픽 대상을 식별하는 그룹을 추가합니다.

c) 개체에 해당 항목을 추가하려면 **Add(**추가**)**를 클릭합니다.

d) 필요한 경우 항목을 클릭한 뒤 위나 아래로 드래그하여 규칙 순서에서 원하는 위치로 이동합니다.

개체에 추가 항목을 생성하거나 편집하려면 프로세스를 반복합니다.

단계 **4** 이 개체에 대한 재정의를 허용하려면 **Allow Overrides(**재정의 허용**)** 확인란을 선택합니다. 개체 재정의 허용, 13 페이지의 내용을 참조하십시오.

단계 **5** **Save(**저장**)**를 클릭합니다.

주소 풀

클러스터링 또는 VPN 원격 액세스 프로파일을 사용해 진단 인터페이스로 사용할 수 있는 IPv4 및 IPv6에 대한 IP 주소 풀을 설정할 수 있습니다.

프로시저

단계 **1** 개체 > 개체 관리 > 주소 풀 > **IPv4** 풀을 선택합니다.

단계 **2** **IPv4** 풀 추가를 클릭하고 다음 필드를 구성합니다.

- **Name(**이름**)** - 주소 풀의 이름을 입력합니다. 최대 64자까지 입력할 수 있습니다.
- **Description(**설명**)** - 필요한 경우 이 풀에 대한 설명을 추가합니다.

- **IP Address(IP** 주소**)** - 풀에서 사용할 수 있는 주소 범위를 입력합니다. 예를 들어 10.10.147.100-10.10.147.177처럼 점으로 구분된 10진수 및 주소 앞뒤 및 사이에 대시를 사용합니다.
- **Mask(**마스크**)** - 이 IP 주소 풀이 있는 서브넷을 식별합니다.
- **Allow Overrides(**오버라이드 허용**)** - 개체 오버라이드를 활성화하려면 이 확인란을 선택합니다. **Overrides(**오버라이드**)** 테이블을 표시하려면 확장 화살표를 클릭합니다. **Add(**추가**)**를 클릭하여 새 오버라이드를 추가할 수 있습니다. 자세한 내용은 개체 재정의, 11 페이지를 참조하십시오.

단계 **3** **Save(**저장**)**를 클릭합니다.

단계 **4** **IPv6** 풀 추가를 클릭하고 다음 필드를 구성합니다.

- **Name(**이름**)** - 주소 풀의 이름을 입력합니다. 최대 64자까지 입력할 수 있습니다.
- **Description(**설명**)** - 필요한 경우 이 풀에 대한 설명을 추가합니다.
- **IPv6 Addres(IPv6** 주소**)** - 구성된 풀에서 사용한 첫 번째 IP 주소 및 접두어 길이를 비트로 입력합니다. 예를 들면 2001:DB8::1 / 64와 같습니다.
- **Number of Addresse(**주소 수**)** - 시작 IP 주소에서 시작하여 풀에 있는 IPv6 주소 수를 식별합니다.
- **Allow Overrides(**오버라이드 허용**)** - 개체 오버라이드를 활성화하려면 이 확인란을 선택합니다. **Overrides(**오버라이드**)** 테이블을 표시하려면 확장 화살표를 클릭합니다. **Add(**추가**)**를 클릭하여 새 오버라이드를 추가할 수 있습니다. 자세한 내용은 개체 재정의, 11 페이지를 참조하십시오.

단계 **5** **Save(**저장**)**를 클릭합니다.

애플리케이션 필터

시스템에서 제공되는 애플리케이션 필터는 유형, 위험, 사업 타당성, 카테고리, 태그라는 기본 특성에 따라 애플리케이션을 구성하여 애플리케이션 컨트롤을 수행할 수 있도록 지원합니다. 개체 관리자에서는 시스템에서 제공되는 필터 조합 또는 사용자 정의 애플리케이션 조합을 기반으로 재사용 가능한 사용자 정의 애플리케이션 필터를 생성 및 관리할 수 있습니다. 자세한 내용은 애플리케이션 규칙 조건를 참조하십시오.

AS 경로

AS 경로는 BGP를 설정하기 위한 필수 속성입니다. 이는 네트워크에 액세스할 수 있는 일련의 AS 번호입니다. AS 경로는 소스와 대상 라우터 간 AS 번호 시퀀스로 패킷이 이동할 방향을 형성합니다. 인접한 자율 시스템(AS)는 BGP를 사용하여 다른 AS 접두사에 도달하는 방법에 대한 메시지를 교환하고 업데이트합니다. 각 라우터가 대상까지 최선의 경로에 대한 새 로컬 결정을 내리면 각 피어에 해당 경로, 경로 정보를 비롯해 거리 메트릭 및 경로 속성을 전송합니다. 이 정보가 네트워크를 통해 이

동할 때 경로의 각 라우터는 고유한 AS 번호를 BGP 메시지의 AS 목록에 첨부합니다. 이 목록은 경로의 AS 경로입니다. AS 접두사가 있는 AS 경로는 네트워크를 통해 단방향 트랜짓 경로에 대한 특정 핸들을 제공합니다. AS 경로 설정 페이지를 사용해 자율 시스템(AS) 경로 정책 개체를 생성, 복사, 편집합니다. 경로 맵, 정책 맵, BGP 네이버 필터링을 구성할 때 사용할 AS 경로 개체를 생성할 수 있습니다. AS 경로 필터를 사용하면 정규식을 사용하여 라우팅 업데이트 메시지를 필터링할 수 있습니다.

이 개체는 threat defense 디바이스와 함께 사용할 수 있습니다.

프로시저

단계 **1** 개체 > 개체 관리를 선택하고 목차에서 **AS** 경로를 선택합니다.

단계 **2** **Add AS Path(AS** 경로 추가**)**를 클릭합니다.

단계 **3** **Name(**이름**)**필드에 AS 경로 개체 이름을 입력합니다. 유효한 값은 1~500입니다.

단계 **4** 새 **AS** 경로 개체 창에서 **Add(**추가**)**를 클릭합니다.

a) 재배포 액세스를 나타내기 위해 작업 드롭다운 목록에서 허용 또는 차단 옵션을 선택합니다.

b) 정규식 필드에 AS 경로 필터를 정의하는 정규식을 지정합니다.

c) **Add(**추가**)**를 클릭합니다.

단계 **5** 이 개체에 대한 재정의를 허용하려면 **Allow Overrides(**재정의 허용**)** 확인란을 선택합니다. 개체 재정의 허용, 13 페이지의 내용을 참조하십시오.

단계 **6** **Save(**저장**)**를 클릭합니다.

암호 그룹 목록

암호 그룹 목록은 여러 암호 그룹으로 구성된 개체입니다. 사전 정의된 각 암호 그룹 값은 SSL 또는 TLS 암호화 세션을 협상하는 데 사용되는 암호 그룹을 나타냅니다. 클라이언트와 서버가 해당 암호 그룹을 사용하여 SSL 세션을 협상했는지 여부를 기반으로 암호화된 트래픽을 제어하기 위해 SSL 규칙의 암호 그룹 및 암호 그룹 목록을 사용할 수 있습니다. SSL 규칙에 암호 그룹 목록을 추가하면 목록의 암호 그룹 중 하나와 협상한 SSL 세션이 규칙을 매칭합니다.

참고 암호 그룹 목록과 동일한 위치에 있는 웹 인터페이스의 암호 그룹을 사용할 수 있지만 암호 그룹을 추가, 수정, 삭제할 수는 없습니다.

암호 그룹 목록 생성

프로시저

단계 **1** **Objects(**개체**)** > **Object Management(**개체 관리**)**을(를) 선택합니다.

단계 **2** 개체 유형 목록에서 **Cipher Suite List(**암호 모음 목록**)**을 선택합니다.

단계 **3** **Add Cipher Suites**를 클릭합니다.

단계 **4** **Name(**이름**)**을 입력합니다.

다중 도메인 구축에서 개체 이름은 도메인 계층 내에서 고유해야 합니다. 시스템은 현재 도메인에서 확인할 수 없는 개체 이름과의 충돌을 식별할 수 있습니다.

단계 **5** **Available Ciphers(**사용 가능한 암호**)** 목록에서 하나 이상의 암호 그룹을 선택합니다.

단계 **6** **Add(**추가**)**를 클릭합니다.

단계 **7** 선택적으로 **Selected Ciphers(**선택한 암호**)** 목록 내 삭제하려는 암호 그룹 옆의 **Delete(**삭제**)** ( )을 클릭합니다.

단계 **8** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

- 활성 정책이 개체를 참조하는 경우 구성 변경 사항을 구축합니다. 참조.

커뮤니티 목록

커뮤니티는 선택적 전이 BGP 속성입니다. 커뮤니티는 공통 속성을 공유하는 목적지 그룹입니다. 경로 태그 지정에 사용됩니다. BGP 커뮤니티 속성은 특정 접두사에 할당되고 다른 네이버에 전달되는 숫자 값입니다. 커뮤니티는 공통 특성을 공유하는 접두사 집합 표시로 사용될 수 있습니다. 업스트림 제공자는 이런 표시를 사용하여 필터링, 특정 로컬 환경설정 할당, 다른 속성 수정 등 일반 라우팅 정책을 적용할 수 있습니다. 커뮤니티 목록 구성 페이지를 사용해 커뮤니티 목록 정책 개체를 생성, 복사, 편집할 수 있습니다. 경로 맵 또는 정책 맵을 구성할 때 사용할 커뮤니티 목록 개체를 생성할 수 있습니다. 커뮤니티 목록을 사용하여 경로 맵의 일치 조항에서 사용할 커뮤니티 그룹을 만들 수 있습니다. 커뮤니티 목록은 일치하는 문장의 순서가 지정된 목록입니다. 일치가 발견될 때까지 규칙을 기준을 대상을 매칭합니다.

이 개체는 threat defense 디바이스와 함께 사용할 수 있습니다.

프로시저

단계 **1** 개체 > 개체 관리를 선택하고 목차에서 커뮤니티 목록을 선택합니다.

단계 **2** **Add Community List(**커뮤니티 목록 추가**)**를 클릭합니다.

단계 **3** 이름 필드에 커뮤니티 목록 개체의 이름을 지정합니다.

단계 **4** 새 커뮤니티 목록 개체 창에서 **Add(**추가**)**를 클릭합니다.

단계 **5** 커뮤니티 규칙 유형을 표시하기 위해 **Standard(**표준**)** 라디오 버튼을 선택합니다.

표준 커뮤니티 목록은 잘 알려진 특정 커뮤니티 또는 커뮤니티 수를 구성하는 데 사용합니다.

참고 표준 커뮤니티 규칙 유형을 사용한 항목과 확장 커뮤니티 규칙 유형을 사용한 항목을 동일한 커뮤니티 목록 개체에 포함시킬 수 없습니다.

a) 재배포 액세스를 나타내기 위해 작업 드롭다운 목록에서 허용 또는 차단 옵션을 선택합니다.
b) **Communities(**커뮤니티**)** 필드에서 커뮤니티 번호를 지정합니다. 유효한 값은 1~4294967295 또는 0:1부터 65534:65535입니다.
c) 적절한 경로 유형을 선택합니다.
   - **Internet(**인터넷**)** - 잘 알려진 인터넷 커뮤니티를 지정하려면 선택합니다. 이 커뮤니티 경로는 모든 피어(내부 및 외부)에게 알려집니다.
   - **No-advertise(**알림 없음**)** - 잘 알려진 커뮤니티의 알림을 하지 않는 경우 선택합니다. 이 커뮤니티 경로는 모든 피어(내부 또는 외부)에게 알려지지 않습니다.
   - **No Export(**내보내지 않음**)** - 잘 알려진 커뮤니티를 내보내지 않는 경우 선택합니다. 이 커뮤니티 경로는 같은 자율 시스템 안에 있는 피어 또는 연합 내에 다른 하위 자율 시스템으로만 알려집니다. 이 경로는 외부 피어에 알려지지 않습니다.

단계 **6** 커뮤니티 규칙 유형을 표시하기 위해 **Expanded(**확장**)** 라디오 버튼을 선택합니다.

확장 커뮤니티 목록은 정규식을 사용하여 커뮤니티를 필터링합니다. 정규식은 커뮤니티 속성과 일치하는 패턴을 지정하는 데 사용됩니다.

a) 재배포 액세스를 나타내기 위해 작업 드롭다운 목록에서 허용 또는 차단 옵션을 선택합니다.
b) 식 필드에 정규식을 지정합니다.

단계 **7** **Add(**추가**)**를 클릭합니다.

단계 **8** 이 개체에 대한 재정의를 허용하려면 **Allow Overrides(**재정의 허용**)** 확인란을 선택합니다. 개체 재정의 허용, 13 페이지의 내용을 참조하십시오.

단계 **9** **Save(**저장**)**를 클릭합니다.

확장 커뮤니티

확장 커뮤니티는 일부 공통 속성을 공유하는 더 큰 대상 그룹입니다. BGP 확장 커뮤니티 목록에는 공통 속성을 공유하는 접두사 세트 표시에 사용할 수 있는 속성이 있습니다. 이러한 표시는 가상 라우터 간의 경로 유출을 구현하기 위해 경로를 필터링하도록 경로 맵의 일치 절에서 사용됩니다. 필터링을 위한 확장 커뮤니티 목록으로 정책 목록 개체를 정의할 수도 있습니다. 확장 커뮤니티 목록은 일치하는 문장의 순서가 지정된 목록입니다. 경로는 지정된 경로 대상(표준) 또는 정규식(확장)과 일치하는 항목이 발견될 때까지 규칙에 대해 일치합니다. 확장 커뮤니티 페이지를 사용하여 커뮤니티 목록 정책 개체를 생성 및 편집합니다.

참고 확장 커뮤니티 목록은 경로 가져오기 또는 내보내기 구성에만 적용됩니다.

이 개체는 threat defense 디바이스와 함께 사용할 수 있습니다.

프로시저

단계 **1** **Objects(**개체**)** > **Object Management(**개체 관리**)**를 선택하고 목차에서 **Community List(**커뮤니티 목록**)** > **Extended Community(**확장 커뮤니티**)**를 선택합니다.

단계 **2** **Add Extended Community List(**확장 커뮤니티 목록 추가**)**를 클릭합니다.

단계 **3** **Name(**이름**)** 필드에 확장 커뮤니티 목록 개체의 이름을 지정합니다. 이름의 길이는 80자를 초과할 수 없습니다.

단계 **4** 확장 커뮤니티 규칙 유형을 선택합니다.

- 하나 이상의 경로 대상을 지정하려면 **Standard(**표준**)** 라디오 버튼을 클릭합니다.
- **Expanded(**확장**)** 라디오 버튼을 클릭하여 정규식을 지정합니다.

참고 동일한 확장 커뮤니티 목록 개체에 Standard(표준) 및 Expanded(확장) 확장 커뮤니티 규칙 유형을 사용한 항목을 포함할 수 없습니다.

단계 **5** **Add(**추가**)**를 클릭합니다.

단계 **6** 확장 커뮤니티 규칙 유형으로 **Standard(**표준**)**를 선택한 경우 다음을 지정합니다.

a) **Sequence No(**시퀀스 번호**)** 필드에 규칙을 실행할 순서를 입력합니다.

시퀀스 번호는 목록에서 고유해야 합니다.

b) **Action(**작업**)** 드롭다운 목록에서 여기에 지정된 경로 대상과 일치하는 경로를 허용하려면 **Allow(**허용**)**를 선택합니다. 여기에 지정된 경로 대상과 일치하는 경로를 거부하려면 **Block(**차단**)**을 선택합니다.

c) **Route Target(**경로 대상**)** 필드에서 경로 대상을 지정합니다.

- 단일 항목에서 단일 경로 대상 또는 쉼표로 구분된 경로 대상 세트를 추가할 수 있습니다. 예: *1:2,1:4,1:6*.
- 유효한 값은 1:1부터 65534:65535입니다.
- 항목에 최대 8개의 경로 대상을 포함할 수 있습니다.
- 여러 항목에 중복 경로 대상 집합이 있을 수 없습니다. 예를 들어 *seq1*을 *1:200,100:100,1:300* 경로 대상으로, *seq2*를 *1:300,100:100,1:200* 경로 대상으로 구성하고자 합니다. 이로 인해 중복 경로 대상 집합이 생성되며 구축할 수 없습니다.

단계 **7** 확장 커뮤니티 규칙 유형으로 **Expanded(**확장**)**를 선택한 경우 다음을 지정합니다.

a) **Sequence No(**시퀀스 번호**)** 필드에 규칙을 실행할 순서를 입력합니다.

시퀀스 번호는 목록에서 고유해야 합니다.

b) **Action(**작업**)** 드롭다운 목록에서 여기에 지정된 정규식과 일치하는 경로를 허용하려면 **Allow(**허용**)**를 선택합니다. 여기에 지정된 정규식과 일치하는 경로를 거부하려면 **Block(**차단**)**을 선택합니다.

c) 식 필드에 정규식을 지정합니다.

- 단일 항목에 단일 경로 대상 또는 공백으로 구분된 경로 대상 집합을 추가할 수 있습니다. *^((16)|(18)):(.)$*를 예로 들 수 있습니다.
- 항목에 최대 16개의 정규식을 추가할 수 있습니다.
- 여러 항목에 중복 정규식 집합이 있을 수 없습니다. 예를 들어 *seq1*을 *^((16)|(18)):(.)$ ^4_[0-9]*$* 경로 대상으로, *seq2*를 *^4_[0-9]*$ ^((16)|(18)):(.)$* 경로 대상으로 구성하고자 합니다. 이로 인해 중복 정규식 집합이 생성되며 구축할 수 없습니다.

BGP 정규식에 대한 자세한 내용은 여기를 참조하십시오.

단계 **8** 이 개체에 대한 재정의를 허용하려면 **Allow Overrides(**재정의 허용**)** 확인란을 선택합니다. 개체 재정의 허용, 13 페이지의 내용을 참조하십시오.

단계 **9** **Save(**저장**)**를 클릭합니다.

확장 커뮤니티 목록은 경로 맵 개체 또는 정책 목록 개체의 일치 절에서 참조할 수 있습니다.

- 경로 맵 개체에서 확장 커뮤니티 목록의 이름이 **Add Route Map Entry(**경로 맵 항목 추가**)** > **Match Clause(**일치 절**)** > **BGP** > **Community List(**커뮤니티 목록**)** > **Add Extended Community List(**확장 커뮤니티 목록 추가**)** 대화 상자에 표시됩니다. 경로 맵에서 BGP 설정 구성에 대한 자세한 내용은 경로 맵, 72 페이지 항목을 참조하십시오.
- 정책 목록 개체에서 확장 커뮤니티 목록의 이름이 **Add Policy List(**정책 목록 추가**)** > **Community Rule(**커뮤니티 규칙**)** > **Add Extended Community List(**확장 커뮤니티 목록 추가**)** 대화 상자에 표시됩니다. 정책 목록에서 BGP 설정 구성에 대한 자세한 내용은 정책 목록, 67 페이지 항목을 참조하십시오.

고유 이름

각 고유 이름(DN) 개체는 공개 키 인증서의 주체 또는 발행자에 대한 고유 이름(DN)을 나타냅니다. 클라이언트 및 서버가 주체 또는 발행자로서 고유 이름과 함께 서버 인증서를 사용하여 TLS/SSL 세션을 협상했는지 여부를 기반으로 암호화된 트래픽을 제어하기 위해 TLS/SSL 규칙 내 고유 이름 개체 및 그룹을 사용할 수 있습니다.

(고유 이름 그룹은 기존 고유 이름 개체의 명명된 컬렉션입니다.)

고유 이름은 국가 코드, 일반 이름, 조직 및 조직 단위로 구성될 수 있지만 일반적으로 공용 이름으로만 구성됩니다. 예를 들어 `https://www.cisco.com`에 대한 인증서의 공통 이름은 `cisco.com`입니다. (그러나 항상 간단한 것은 아닙니다. 고유 이름(DN) 규칙 조건에서는 공통 이름을 찾는 방법을 보여줍니다.) 인증서에는 규칙 조건에서 DN으로 사용할 수 있는 여러 SAN(주체 대체 이름)이 포함될 수 있습니다. SAN에 대한 자세한 내용은 RFC 5280, 섹션 4.2.1.6을 참조하십시오.

공통 이름을 참조하는 고유 이름 개체의 형식은 `CN= name`입니다. `CN=` 없이 DN 규칙 조건을 추가하면 개체를 저장하기 전에 시스템이 `CN=`을 앞에 추가합니다.

고유 이름(DN) 규칙 조건에서 자세히 설명하는 것처럼, 시스템은 가능한 경우 항상 SNI(서버 이름 표시)를 사용하여 TLS/SSL 규칙의 DN을 일치시킵니다.

다음 표에 나열된 각 속성 중 하나와 함께 쉼표로 구분하여 고유 이름(DN)을 추가할 수 있습니다.

표 *1:* 고유 이름 속성

속성	설명	허용 값
전체	국가 코드	영문자 2개
CN	공용 이름(CN)	최대 64자의 영숫자, 백슬래시(/), 하이픈(-), 따옴표("), 별표(*) 문자 또는 공백
O	조직	최대 64자의 영숫자, 백슬래시(/), 하이픈(-), 따옴표("), 별표(*) 문자 또는 공백
OU	조직 단위	최대 64자의 영숫자, 백슬래시(/), 하이픈(-), 따옴표("), 별표(*) 문자 또는 공백

DN 규칙 조건에 대한 중요 참고 사항

- 시스템이 새 서버로의 암호화된 세션을 처음 탐지할 때는 ClientHello 처리에 DN 데이터를 사용할 수 없으므로 첫 번째 세션이 암호 해독되지 않습니다.

  서버가 TLS 1.3을 요청하는 경우, TLS 서버 ID 검색을 위한 설정은 SSL 정책 결정을 내리기 전에 서버 인증서가 알려졌는지 확인하는 데 도움이 될 수 있습니다. 자세한 내용은 액세스 제어 정책 고급 설정를 참고하십시오.

- **Decrypt - Known Key(**암호 해독 - 알려진 키**)** 작업도 선택할 경우 고유 이름(DN) 조건을 구성할 수 없습니다. 이 작업은 서버 인증서 선택을 통한 트래픽 해독이 필요하므로 인증서가 트래픽과 이미 일치합니다.

와일드카드 예

속성에서 하나 이상의 별표(*)를 와일드카드로 정의할 수 있습니다. 공용 이름 속성에서 도메인 이름 레이블당 하나 이상의 별표를 정의할 수 있습니다. 와일드카드는 해당 레이블에서만 일치하지만 와일드카드를 사용하여 여러 레이블을 정의할 수 있습니다. 다음 표의 예를 참고하십시오.

표 *2:* 공용 이름 속성 와일드카드 예

특성	일치	일치하지 않음
CN=*ample.com	example.com	mail.example.com example.text.com ampleexam.com
CN=exam*.com	example.com	mail.example.com example.text.com ampleexam.com

특성	일치	일치하지 않음
CN=*xamp*.com	example.com	mail.example.com example.text.com ampleexam.com
CN=*.example.com	mail.example.com	www.myhost.example.com example.com example.text.com ampleexam.com

참고 DN 개체 `CN=amp.cisco.com`은 `CN=auth.amp.cisco.com`과 같은 CN과 일치하지 않으므로 이러한 경우 와일드카드를 사용하는 것이 좋습니다.

추가 정보 및 예시는 고유 이름(DN) 규칙 조건의 내용을 참조하십시오.

관련 항목

고유 이름(DN) 규칙 조건

고유 이름(DN) 개체 생성

프로시저

단계 **1** **Objects**(개체) > **Object Management**(개체 관리)을(를) 선택합니다.

단계 **2** **Distinguished Name**(고유 이름) 노드를 확장하고 **Individual Objects**(개별 개체)를 선택합니다.

단계 **3** **Add Distinguished Name**(고유 이름(DN) 추가)을 클릭합니다.

단계 **4** **Name**(이름)을 입력합니다.

다중 도메인 구축에서 개체 이름은 도메인 계층 내에서 고유해야 합니다. 시스템은 현재 도메인에서 확인할 수 없는 개체 이름과의 충돌을 식별할 수 있습니다.

단계 **5** **DN** 필드에 고유 이름 또는 공통 이름의 값을 입력합니다. 다음 옵션을 이용할 수 있습니다.

- 고유 이름(DN)을 추가하면 고유 이름, 29 페이지에 나열된 각 특성 중 하나를 쉼표로 구분하여 포함할 수 있습니다.
- 공용 이름(CN)을 추가하는 경우 여러 레이블과 와일드카드를 포함할 수 있습니다.

단계 **6** **Save**(저장)를 클릭합니다.

다음에 수행할 작업

- 활성 정책이 개체를 참조하는 경우 구성 변경 사항을 구축합니다. 참조.

DNS 서버 그룹

DNS(Domain Name System) 서버는 www.example.com 같은 FQDN(Fully Qualified Domain Name)을 IP 주소로 확인합니다.

DNS 서버 그룹 개체 생성

프로시저

단계 **1** **Objects(**개체**)** > **Object Management(**개체 관리**)**를 선택합니다.

단계 **2** 네트워크 개체 목록에서 **DNS Server Group(DNS** 서버 그룹**)**을 클릭합니다.

단계 **3** **Add DNS Server Group(DNS** 서버 그룹 추가**)**을 클릭합니다.

단계 **4** **Name(**이름**)**을 입력합니다.

다중 도메인 구축에서 개체 이름은 도메인 계층 내에서 고유해야 합니다. 시스템은 현재 도메인에서 확인할 수 없는 개체 이름과의 충돌을 식별할 수 있습니다.

단계 **5** 필요에 따라 정규화되지 않은 호스트 이름에 추가하는 데 사용될 기본 도메인을 입력합니다.

이 설정은 기본 서버 그룹에만 사용됩니다.

단계 **6** 기본 시간 초과 및 재시도 값은 사전 입력되어 있습니다. 필요한 경우 이 값을 변경합니다.

- Retries(재시도 횟수) - 시스템이 응답을 받지 못한 경우 DNS 서버 목록을 재시도할 횟수(0~10회)입니다. 기본값은 2입니다.
- Timeout(시간한) — 다음 DNS 서버를 시도하기 전에 기다리는 시간(1~30초)입니다. 기본값은 2초입니다. 시스템이 서버 목록을 재시도할 때마다 이 시간 초과 값이 두 배로 늘어납니다.

단계 **7** 쉼표로 구분된 항목으로 IPv4 또는 IPv6 형식으로 이 그룹의 일부가 될 **DNS** 서버를 입력합니다.

하나의 그룹에 최대 6개의 DNS 서버가 포함될 수 있습니다.

단계 **8** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

DNS 서버 그룹의 DNS 서버 구성은 DNS 플랫폼 설정의 인터페이스 개체에 할당되어야 합니다. 자세한 내용은 DNS 구성를 참고하십시오.

외부 특성

동적 개체

동적 개체는 IP 또는 Cisco Secure Dynamic Attributes Connector를 사용하여 생성할 수 있는 개체입니다. 이 통합은 클라우드 네트워킹 제품의 개체를 management center 액세스 제어 규칙에서 사용할 수 있도록 하는 통합입니다.

동적 속성 커넥터에 대한 자세한 내용은 이 가이드의 뒷부분에 있는 정보를 참조하십시오.

동적 개체와 네트워크 개체의 차이점은 다음과 같습니다.

- 동적 속성 커넥터를 사용하여 생성된 동적 개체는 생성되는 즉시 management center에 푸시되며 정기적인 간격으로 업데이트됩니다.
- API가 생성한 동적 개체:
  - 네트워크 개체와 매우 유사하게 액세스 제어 규칙에서 사용할 수 있는 CIDR(Classless Inter-Domain Routing)이 있거나 없는 IP 주소입니다.
  - 정규화된 도메인 이름 또는 주소 범위를 지원하지 않습니다.
  - API를 사용하여 업데이트해야 합니다.

관련 항목

동적 개체 추가 또는 편집, 33 페이지

동적 개체 추가 또는 편집

이 절차에서는 네트워크 개체와 매우 유사하게 액세스 제어 규칙에서 사용할 수 있는 *CIDR*(Classless Inter-Domain Routing)을 사용하거나 사용하지 않는 IP 주소 그룹인 동적 개체를 API를 사용하여 추가하거나 수정하는 방법을 설명합니다.

참고 Cisco Secure Dynamic Attributes Connector를 사용하는 경우에는 동적 개체가 자동으로 생성되므로 이 절차는 필요하지 않습니다.

시작하기 전에

개체 서비스 API를 사용하여 IP 개체에 주소를 입력하는 방법에 대한 자세한 내용은 *Firepower Management Center REST API Quick Start Guide*를 참조하십시오. 동적 개체는 구축할 필요가 없습니다.

프로시저

단계 **1** **Objects(**개체**)** > **Object Management(**개체 관리**)** 버튼을 클릭합니다.

단계 **2** **External Attributes(**외부 속성**)** > **Dynamic Objects(**동적 개체**)**를 클릭합니다.

단계 **3** **Add Dynamic Object(**동적 개체 추가**)**를 클릭하거나 **Edit(**수정**)** ( ).

단계 **4** 개체의 **Name(**이름**)** 및 **Description(**설명**)**(선택 사항)을 입력합니다.

단계 **5** **Type(**유형**)** 목록에서 **IP**를 클릭합니다.

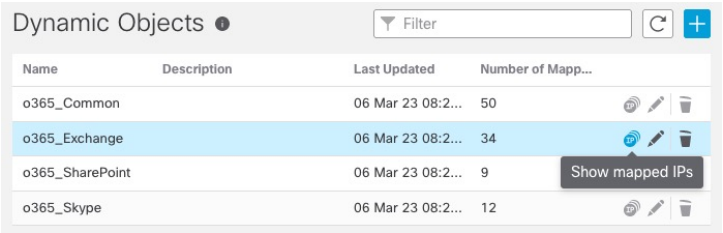
다음에 수행할 작업

필요한 경우 API를 사용하여 동적 개체를 업데이트합니다. 구축이 필요하지 않습니다.

동적 개체 매핑

API 또는 동적 속성 커넥터를 사용하여 동적 개체를 구성한 경우, 커넥터는 동적 특성 필터와 일치하는 IP를 management center에 정기적으로 전송합니다.

이러한 IP 주소의 현재 목록을 보거나 다운로드하려면 다음 그림과 같이 **Show Mapped IDs(**매핑된 **ID** 표시**)**를 클릭합니다.



IP 주소는 시간이 지남에 따라 동적으로 추가되므로 특히 액세스 제어 규칙이 예상대로 작동하지 않는 경우 이 작업을 정기적으로 수행하는 것이 좋습니다.

관련 항목

- 동적 개체, 33 페이지

Security Group Tag(보안 그룹 태그)

SGT(Security Group Tag) 개체는 단일 SGT 값을 지정합니다. Cisco ISE가 할당하지 않은 SGT 속성으로 트래픽을 제어하기 위해 규칙에서 SGT 개체를 사용할 수 있습니다. SGT 개체는 그룹화 또는 재정의할 수 없습니다.

관련 항목

사용자 정의 SGT에서 ISE SGT로 자동 전환
맞춤형 SGT 조건
ISE SGT 및 맞춤형 SGT 규칙 조건 비교

보안 그룹 태그 개체 생성

전역 도메인에서만 이러한 개체를 생성할 수 있습니다. 클래식 디바이스에서 개체를 사용하려면 제어 라이센스가 있어야 합니다. Smart Licensed 디바이스의 경우 모든 라이센스가 적용됩니다.

시작하기 전에

- ISE/ISE-PIC 연결을 비활성화합니다. ID 소스로 ISE/ISE-PIC를 사용하는 경우 사용자 정의 SGT 개체를 생성할 수 없습니다.

프로시저

단계 **1** **Objects(**개체**)** > **Object Management(**개체 관리**)** 버튼을 클릭합니다.

단계 **2** **External Attributes(**외부 속성**)** > **Dynamic Objects(**동적 개체**)**를 클릭합니다.

단계 **3** **Add Security Group Tag(**보안 그룹 태그 추가**)**를 클릭합니다.

단계 **4** **Name(**이름**)**을 입력합니다.

단계 **5** 필요한 경우 **Description(**설명**)**을 입력합니다.

단계 **6** **Tag(**태그**)** 필드에 단일 SGT를 입력합니다.

단계 **7** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

- 활성 정책이 개체를 참조하는 경우 구성 변경 사항을 구축합니다. 참조.

파일 목록

악성코드 대응 를 사용하고 AMP 클라우드가 파일의 속성을 잘못 식별하는 경우 향후 파일을 더 잘 탐지하기 위해 파일 목록에 파일을 추가할 수 있습니다. 이러한 파일은 SHA-256 해시 값을 사용해 지정됩니다. 각 파일 목록은 최대 10000개의 고유한 SHA-256 값을 포함할 수 있습니다.

파일 목록에는 두 개의 사전 정의된 카테고리가 있습니다.

안전 목록

이 목록에 파일을 추가하는 경우 시스템은 AMP 클라우드가 파일을 안전 속성으로 할당했다고 간주합니다.

사용자 지정 탐지 목록

이 목록에 파일을 추가하는 경우 시스템은 AMP 클라우드가 악성코드 속성으로 할당했다고 간주합니다.

다중 도메인 구축 시 안전 목록 및 사용자 지정 탐지 목록은 각 도메인마다 표시됩니다. 하위 도메인에서는 볼 수 있지만 상위 도메인의 항목은 수정할 수 없습니다.

이 목록에 포함된 파일에 대한 차단을 수동으로 지정하므로 시스템은 이런 파일의 속성에 대해 AMP 클라우드에 쿼리하지 않습니다. 파일 정책을 구성할 때는 **Malware Cloud Lookup(**악성코드 클라우드 조회**)** 또는 **Block Malware(**악성코드 차단**)** 작업 중 하나 및 파일의 SHA 값을 계산하는 일치 파일 유형을 포함한 규칙을 구성해야 합니다.

⚠

주의 안전 목록에 악성코드를 포함하지 마십시오. 안전 목록은 AMP 클라우드 및 사용자 지정 탐지 목록에 오버라이드됩니다.

파일 목록에 대한 소스 파일

SHA-256 값 및 설명이 포함된 쉼표로 구분된 값(CSV) 소스 파일을 업로드하여 파일 목록에 복수의 SHA-256 값을 추가할 수 있습니다. management center은 콘텐츠를 확인하고 파일 목록에 유효한 SHA-256 값을 입력합니다.

소스 파일은 .csv 파일 이름 확장자를 가진 간편한 텍스트 파일이어야 합니다. 모든 헤더는 파운드 기호(#)로 시작해야 합니다. 이는 코멘트로 처리되어 업로드되지 않습니다. 각 항목은 LF 또는 CR+LF 줄 바꿈 문자로 끝나며 설명이 있는 단일 SHA-256 값을 포함해야 합니다. 시스템은 항목의 추가 정보는 모두 무시합니다.

다음 사항을 참고하십시오.

- 파일 목록에서 소스 파일을 삭제하면 이는 또한 파일 목록에서 모든 관련 SHA-256 해시를 제거합니다.
- 성공적인 소스 파일 업로드의 결과 파일 목록이 10000개 이상의 명시적 SHA-256 값을 포함하는 경우 파일 목록에 여러 파일을 업로드할 수 없습니다.
- 시스템은 업로드 시 256개의 문자를 초과하는 설명이 있으면 이를 줄여서 처음 256개 문자만 남깁니다. 설명에 쉼표가 포함되어 있는 경우, 이스케이프 문자(\,)를 사용해야 합니다. 어떤 설명도 포함되지 않은 경우, 소스 파일 이름을 대신 사용합니다.
- 모든 비복제 SHA-256 값이 파일 목록에 추가됩니다. 파일 목록이 SHA-256 값을 포함하고 해당 값이 포함된 소스 파일을 업로드할 경우, 새로 업로드한 값은 기존 SHA-256 값을 변경하지 않습니다. 캡처 파일, 파일 이벤트 또는 SHA-256 값과 관련된 악성코드 이벤트를 볼 때, 모든 위협 이름 또는 설명은 개별 SHA-256 값에서 파생됩니다.
- 시스템은 소스 파일에 유효하지 않은 SHA-256 값을 업로드하지 않습니다.
- 업로드된 여러 소스 파일이 동일한 SHA-256 값에 대한 항목을 포함할 경우 시스템은 가장 최근 값을 사용합니다.
- 소스 파일이 동일한 SHA-256 값에 대한 여러 항목을 포함할 경우, 시스템은 가장 최근 값을 사용합니다.
- 개체 관리자 내 소스 파일을 직접 수정할 수 없습니다. 변경하려면, 먼저 소스 파일을 직접 수정하고, 시스템에서 복사본을 삭제한 후, 수정된 소스 파일을 업로드해야 합니다.

- 소스 파일과 관련된 항목 수는 명시적 SHA-256 값의 수를 나타납니다. 파일 목록에서 소스 파일을 삭제하는 경우, 파일 목록이 포함하는 SHA-256 항목의 총 수는 소스 파일 내 유효한 항목 수에 따라 감소합니다.

파일 목록에 개별 **SHA-256** 값 추가

이 절차를 수행하려면 악성코드 라이선스가 있어야 합니다.

파일의 SHA-256 값을 제출하여 파일 목록에 추가할 수 있습니다. 중복된 SHA-256 값은 추가할 수 없습니다.

다중 도메인 구축에서 시스템은 현재 도메인에서 생성된 개체를 표시하며 이러한 개체는 수정할 수 있습니다. 상위 도메인에서 생성된 개체도 표시되지만, 이러한 개체는 수정할 수 없습니다. 하위 도메인에서 생성된 개체를 보고 수정하려면 해당 도메인으로 전환하십시오.

시작하기 전에

- 이벤트 보기에서 파일 또는 악성코드 이벤트를 오른쪽 클릭하고 컨텍스트 메뉴에서 **Show Full Text(**전체 텍스트 보기**)**를 선택하여 파일 항목에 붙여넣기 할 전체 SHA-256 값을 복사합니다.

프로시저

단계 **1** **Objects(**개체**)** > **Object Management(**개체 관리**)**을(를) 선택합니다.

단계 **2** 개체 유형 목록에서 **File List(**파일 목록**)**을 선택합니다.

단계 **3** 파일을 추가하려는 정상 목록 또는 사용자 정의 탐지 목록 옆의 **Edit(**수정**)** ( )을 클릭합니다.

View(보기**)** ( )가 대신 표시되는 경우에는 개체가 상위 도메인에 속하거나 개체를 수정할 권한이 없는 것입니다.

단계 **4** 드롭다운 목록에서 **Add by(**추가 기준**)**의 `Enter SHA Value(SHA 값 입력)`를 선택합니다.

단계 **5** **Description(**설명**)** 필드에 소스 파일에 대한 설명을 입력합니다.

단계 **6** 파일의 전체 값을 **SHA-256** 필드에 입력하거나 붙여 넣습니다. 시스템은 일치하는 부분 값을 지원하지 않습니다.

단계 **7** **Add(**추가**)**를 클릭합니다.

단계 **8** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

- 활성 정책이 개체를 참조하는 경우 구성 변경 사항을 구축합니다. 참조.

참고 설정 변경을 구축한 뒤 시스템은 목록의 파일에 대한 AMP 클라우드를 더 이상 쿼리하지 않습니다.

파일 목록에 개별 파일 업로드

이 절차를 수행하려면 악성코드 라이선스가 있어야 합니다.

파일 목록에 추가하려는 파일의 사본이 있는 경우 분석을 위해 Secure Firewall Management Center에 파일을 업로드할 수 있습니다. 시스템은 파일의 SHA-256 값을 계산하고 목록에 파일을 추가합니다. 시스템은 SHA-256 계산을 위한 파일 크기에 제한을 두지 않습니다.

다중 도메인 구축에서 시스템은 현재 도메인에서 생성된 개체를 표시하며 이러한 개체는 수정할 수 있습니다. 상위 도메인에서 생성된 개체도 표시되지만, 이러한 개체는 수정할 수 없습니다. 하위 도메인에서 생성된 개체를 보고 수정하려면 해당 도메인으로 전환하십시오.

프로시저

단계 **1** **Objects(**개체**)** > **Object Management(**개체 관리**)**을(를) 선택합니다.

단계 **2** 개체 유형 목록에서 **File List(**파일 목록**)**을 선택합니다.

단계 **3** 파일을 추가하려는 정상 목록 또는 사용자 정의 탐지 목록 옆의 **Edit(**수정**)** ( )을 클릭합니다.

View(보기**)** ( )가 대신 표시되는 경우에는 개체가 상위 도메인에 속하거나 개체를 수정할 권한이 없는 것입니다.

단계 **4** 드롭다운 목록의 **Add(**추가**)**에서 **Calculate SHA(SHA** 계산**)**을 선택합니다.

단계 **5** 또는, **Description(**설명**)** 필드에 파일에 대한 설명을 입력합니다. 설명을 입력하지 않은 경우, 업로드 시 설명에 파일 이름이 사용됩니다.

단계 **6** **Browse(**탐색**)**를 클릭하여 업로드할 파일을 선택합니다.

단계 **7** **Calculate and Add SHA(SHA** 계산 및 추가**)**를 클릭합니다.

단계 **8** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

- 활성 정책이 개체를 참조하는 경우 구성 변경 사항을 구축합니다. 참조.

참고 설정 변경을 구축한 뒤 시스템은 목록의 파일에 대한 AMP 클라우드를 더 이상 쿼리하지 않습니다.

파일 목록에 소스 파일 업로드

이 절차를 수행하려면 악성코드 라이선스가 있어야 합니다.

다중 도메인 구축에서 시스템은 현재 도메인에서 생성된 개체를 표시하며 이러한 개체는 수정할 수 있습니다. 상위 도메인에서 생성된 개체도 표시되지만, 이러한 개체는 수정할 수 없습니다. 하위 도메인에서 생성된 개체를 보고 수정하려면 해당 도메인으로 전환하십시오.

프로시저

단계 **1** **Objects(**개체**)** > **Object Management(**개체 관리**)**을(를) 선택합니다.

단계 **2** **File List(**파일 목록**)**를 클릭합니다.

단계 **3** 소스 파일의 값을 추가할 파일 목록 옆에 있는 **Edit(**수정**)** ( )을 클릭합니다.

View(보기**)** ( )가 대신 표시되는 경우에는 개체가 상위 도메인에 속하거나 개체를 수정할 권한이 없는 것입니다.

단계 **4** 드롭다운 목록의 **Add(**추가**)**에서 `List of SHAs(SHA 목록)`을 선택합니다.

단계 **5** 또는, **Description(**설명**)** 필드에 소스 파일에 대한 설명을 입력합니다. 설명을 입력하지 않을 경우, 시스템은 파일 이름을 사용합니다.

단계 **6** **Browse(**찾아보기**)**를 클릭하여 소스 파일을 탐색한 후 **Upload and Add List(**목록 업로드 및 추가**)**를 클릭합니다.

단계 **7** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

- 활성 정책이 개체를 참조하는 경우 구성 변경 사항을 구축합니다. 참조.

참고 정책을 구축한 후 시스템은 목록의 파일에 대한 AMP 클라우드를 더 이상 쿼리하지 않습니다.

파일 목록에서 **SHA-256** 값 수정

이 절차를 수행하려면 악성코드 라이선스가 있어야 합니다.

파일 목록에서 개별 SHA-256 값을 편집하거나 삭제할 수 있습니다. 개체 관리자 내 소스 파일을 직접 수정할 수 없다는 점에 유의하십시오. 변경하려면, 먼저 소스 파일을 직접 수정하고, 시스템에서 복사본을 삭제한 후, 수정된 소스 파일을 업로드해야 합니다.

다중 도메인 구축에서 시스템은 현재 도메인에서 생성된 개체를 표시하며 이러한 개체는 수정할 수 있습니다. 상위 도메인에서 생성된 개체도 표시되지만, 이러한 개체는 수정할 수 없습니다. 하위 도메인에서 생성된 개체를 보고 수정하려면 해당 도메인으로 전환하십시오.

프로시저

단계 **1** **Objects(**개체**)** > **Object Management(**개체 관리**)**을(를) 선택합니다.

단계 **2** **File List(**파일 목록**)**를 클릭합니다.

단계 **3** 수정하려는 파일이 포함된 정상 목록 또는 사용자 정의 탐지 목록 옆의 **Edit(**수정**)** ( )을 클릭합니다.

View(보기**)** ( )가 대신 표시되는 경우에는 개체가 상위 도메인에 속하거나 개체를 수정할 권한이 없는 것입니다.

단계 **4** 다음 작업을 수행할 수 있습니다.

- 변경하려는 SHA-256 값 옆의 **Edit(**수정**)** ( )을 클릭하고 원하는 **SHA-256** 또는 설명 값을 수정합니다.
- 삭제할 SHA-256 값 옆의 **Delete(**삭제**)** ( )을 클릭합니다.

단계 **5** 목록에서 파일 항목을 업데이트하려면 **Save(**저장**)**을 클릭합니다.

단계 **6** **Save(**저장**)**를 클릭하여 파일 목록을 저장합니다.

다음에 수행할 작업

- 활성 정책이 개체를 참조하는 경우 구성 변경 사항을 구축합니다. 참조.

참고 설정 변경을 구축한 뒤 시스템은 목록의 파일에 대한 AMP 클라우드를 더 이상 쿼리하지 않습니다.

파일 목록에서 소스 파일 다운로드

이 절차를 수행하려면 악성코드 라이선스가 있어야 합니다.

다중 도메인 구축에서 시스템은 현재 도메인에서 생성된 개체를 표시하며 이러한 개체는 수정할 수 있습니다. 상위 도메인에서 생성된 개체도 표시되지만, 이러한 개체는 수정할 수 없습니다. 하위 도메인에서 생성된 개체를 보고 수정하려면 해당 도메인으로 전환하십시오.

프로시저

단계 **1** **Objects(**개체**)** > **Object Management(**개체 관리**)**을(를) 선택합니다.

단계 **2** 개체 유형 목록에서 **File List(**파일 목록**)**을 선택합니다.

단계 **3** 소스 파일을 다운로드하려는 정상 목록 또는 사용자 정의 탐지 목록 옆의 **Edit(**수정**)** ( )을 클릭합니다.

View(보기**)** ( )가 대신 표시되는 경우에는 개체가 상위 도메인에 속하거나 개체를 수정할 권한이 없는 것입니다.

단계 **4** 다운로드할 소스 파일 옆에 있는 **View(**보기**)** ( )을 클릭합니다.

단계 **5** **Download SHA List(SHA** 목록 다운로드**)**를 클릭하고 프롬프트에 따라 소스 파일을 저장합니다.

단계 **6** **Close(**닫기**)**를 클릭합니다.

FlexConfig

threat defense 디바이스에서 사용할 수 없는 사용자 정의 설정 기능을 제공하려면 FlexConfig 정책에서 FlexConfig 정책 개체를 사용하거나 Secure Firewall Management Center를 사용해 구성합니다. FlexConfig 정책에 대한 자세한 내용은 FlexConfig 정책 개요을 참조하십시오.

FlexConfig에 대한 다음과 같은 유형의 개체를 구성할 수 있습니다.

텍스트 개체

텍스트 개체는 FlexConfig 개체에서 변수로 사용하는 자유 형식의 텍스트 문자열을 정의합니다. 이러한 개체는 단일 값을 가질 수도 있고 여러 값의 목록일 수도 있습니다.

사전 정의된 FlexConfig 개체에서 사용되는 몇 가지 사전 정의된 텍스트 개체가 있습니다. 연결된 FlexConfig 개체를 사용하는 경우에 해당 디바이스에 FlexConfig 개체를 구성하는 방법을 사용자 정의하려면 텍스트 개체의 내용을 편집하면 됩니다. 사전 정의된 개체를 편집할 때 일반적으로 해당 개체의 기본값을 직접 변경하는 것보다 구성하는 각 디바이스에 디바이스 오버라이드를 생성하는 것이 더 낫습니다. 이렇게 하면 다른 사용자가 디바이스의 다른 집합에 동일한 FlexConfig 개체를 사용하려는 경우 예기치 않은 결과가 발생하는 것을 방지합니다.

텍스트 개체를 구성하는 방법에 대해서는 FlexConfig 텍스트 개체 설정을 참조하십시오.

FlexConfig 개체

FlexConfig 개체는 디바이스 설정 명령, 변수 및 스크립팅 언어 지침을 포함합니다. 설정을 구축하는 동안 대상 디바이스에 대해 특정 기능을 구성하기 위해 사용자 정의된 파라미터를 포함한 일련의 설정 명령어를 생성하기 위해 지침이 처리됩니다.

이러한 지침은 일반 management center 정책 및 설정에서 시스템 구성 기능이 정의되기 전(앞)에 구성되거나 후(뒤)에 구성됩니다. Secure Firewall Management Center에 의존하는 모든 FlexConfig - 구성 구축에 구성된 개체(네트워크 개체 등)를 추가하지 않으면 FlexConfig가 개체 참조에 사용하기 전에 필요한 개체가 구성되지 않습니다.

FlexConfig 개체를 구성하는 방법에 대해서는 FlexConfig 개체 구성을 참조하십시오.

지리위치

사용자가 구성한 각 지리위치 개체는 시스템이 사용자의 모니터링된 네트워크에서 트래픽의 소스 또는 대상으로 파악한 하나 이상의 국가 또는 대륙을 나타냅니다. 액세스 제어 정책, SSL 정책, 이벤트 검색 등 시스템 웹 인터페이스의 여러 위치에서 지리위치 개체를 사용할 수 있습니다. 예를 들어, 특정 국가를 오가는 트래픽을 차단하는 액세스 제어 규칙을 작성할 수 있습니다.

네트워크 트래픽을 필터링하기 위해 최신 정보를 사용하려면 정기적으로 지리위치 데이터베이스(GeoDB)를 업데이트할 것을 강력하게 권장합니다.

지리위치 개체 생성

프로시저

단계 **1** **Objects(**개체**)** > **Object Management(**개체 관리**)**을(를) 선택합니다.

단계 **2** 개체 유형 목록에서 **Geolocation(**지리위치**)**를 선택합니다.

단계 **3** **Add Geolocation(**지리위치 추가**)**을 클릭합니다.

단계 **4** **Name(**이름**)**을 입력합니다.

다중 도메인 구축에서 개체 이름은 도메인 계층 내에서 고유해야 합니다. 시스템은 현재 도메인에서 확인할 수 없는 개체 이름과의 충돌을 식별할 수 있습니다.

단계 **5** 지리위치 개체에 포함할 국가와 대륙의 확인란을 선택합니다. 대륙을 선택하면 해당 대륙 내의 모든 국가와 GeoDB 업데이트가 향후 해당 대륙에 추가하는 모든 국가를 선택합니다. 대륙에 속한 모든 국가를 선택 취소하려면 대륙을 선택 취소합니다. 국가 및 대륙의 모든 조합을 선택할 수 있습니다.

단계 **6** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

- 활성 정책이 개체를 참조하는 경우 구성 변경 사항을 구축합니다. 참조.

Interface(인터페이스)

각 인터페이스는 보안 영역 및/또는 인터페이스 그룹에 할당될 수 있습니다. 영역 또는 그룹을 기준으로 보안 정책을 적용합니다. 예를 들어, "내부" 인터페이스는 "내부" 영역에, "외부" 인터페이스는 "외부" 영역에 할당할 수 있습니다. 예를 들어, 트래픽이 내부에서 외부로는 이동하되 외부에서 내부로는 이동할 수 없도록 액세스 제어 정책을 구성할 수 있습니다. 일부 정책은 보안 영역만 지원하고 일부 정책은 영역 및 그룹을 지원합니다.

인터페이스 개체에 대한 자세한 내용은 보안 영역 및 인터페이스 그룹의 내용을 참조하십시오.

인터페이스 개체를 추가하려면 보안 영역 및 인터페이스 그룹 개체 생성의 내용을 참조하십시오.

키 체인

데이터 보안 및 디바이스 보호 기능을 강화하기 위해 IGP 피어 인증용 회전 키는 최대 180일간 사용할 수 있습니다. 회전 키는 악의적인 사용자가 라우팅 프로토콜 인증에 사용되는 키를 추측하는 것을 방지하므로 네트워크가 잘못된 경로를 알리고 트래픽을 리디렉션하지 못하도록 보호합니다. 키를 자주 변경하면 결국에는 추측되는 위험이 줄어듭니다. 키 체인을 제공하는 라우팅 프로토콜에 대한 인증을 구성할 때 키 체인의 키 수명이 겹치도록 구성합니다. 이렇게 하면 액티브 키가 없기 때문에 키 보안 통신이 손실되는 것을 방지하는 데 도움이 됩니다. 회전 키는 OSPFv2 프로토콜에만 적용될

수 있습니다. 키 수명이 만료되고 액티브 키를 찾을 수 없는 경우 OSPF는 피어와의 인접성을 유지 관리하기 위해 마지막으로 유효한 키를 사용합니다.

참고 인증에는 MD5 암호화 알고리즘만 사용됩니다.

키 수명

안정적인 통신을 유지하기 위해 각 디바이스는 키 체인 인증 키를 저장하고 동시에 한 개 이상의 키를 사용합니다. 키 체인 관리는 키 전송 및 수신 수명을 기반으로 키의 롤오버를 처리하는 보안 메커니즘을 제공합니다. 디바이스는 키의 수명을 사용해 키 체인에서 활성화될 키를 결정합니다.

키 체인의 각 키에는 두 개의 수명이 있습니다.

- 수신 수명 - 다른 디바이스와 키를 교환할 때 디바이스가 키를 수신하는 데 걸리는 시간 간격입니다.
- 전송 수명 - 다른 디바이스와 키를 교환할 때 디바이스가 키를 전송하는 데 걸리는 시간 간격입니다.

키 전송 수명 동안 디바이스는 키로 라우팅 업데이트 패킷을 전송합니다. 디바이스는 전송된 키가 디바이스의 키 수신 수명을 벗어난 경우 다른 디바이스의 통신을 수신하지 않습니다.

키 수명이 구성되지 않은 경우 타임라인 없이 MD5 인증 키를 구성하는 것과 같습니다.

키 선택

- 키 체인에 하나 이상의 유효한 키가 있는 경우 OSPF는 최대 수명을 가지고 있는 키를 선택합니다.
- 키의 수명은 무한인 것이 좋습니다.
- 키가 동일한 수명을 가진 경우 키 ID가 높은 키가 좋습니다.

키 체인 개체 생성

프로시저

단계 **1** **Objects(**개체**)** > **Object Management(**개체 관리**)**을(를) 선택합니다.

단계 **2** 개체 유형 목록에서 **Key Chain(**키 체인**)**을 선택합니다.

단계 **3** **Add Key Chain(**키 체인 추가**)**를 클릭합니다.

단계 **4** 키 체인 개체 추가 대화 상자의 이름 필드에 키 체인의 이름을 입력합니다.

이름은 밑줄 또는 알파벳으로 시작해야 하며 이후에는 영숫자 및 특수 문자(-, _, +, .)로 구성되어야 합니다.

단계 **5** 키 체인에 키를 추가하려면 **Add(**추가**)**를 클릭합니다.

단계 **6** **Key ID** 필드에 키 식별자를 지정합니다.

키 ID 값은 0~255 범위의 값일 수 있습니다. 유효하지 않은 키를 표시하려는 경우에만 0을 사용합니다.

단계 **7** 알고리즘 필드 및 암호화 유형 필드는 MD5 및 일반 텍스트로 지원되는 알고리즘 및 암호화 유형을 표시합니다.

단계 **8** 암호화 키 문자열 필드에 암호를 입력하고 암호화 키 문자열 확인 필드에 암호를 다시 입력합니다.

- 암호의 길이는 최대 80자입니다.
- 한 자리 숫자이거나 숫자 뒤에 공백이 오는 암호는 지정할 수 없습니다. 예를 들어 "0 pass" 또는 "1"은 유효하지 않습니다.

단계 **9** 다른 디바이스와 키 교환 시 키를 수신/전송하는 시간 간격을 설정하려면 수신 수명 및 전송 수명 필드에 수명 값을 제공합니다.

참고 날짜 및 시간 값은 UTC 표준 시간대를 기본으로 사용합니다.

종료 시간은 수신/전송 수명이 종료되거나 영원히 만료되지 않는 경우의 기간, 즉 절대 시간이 될 수 있습니다. 기본 종료 시간은 날짜 및 시간입니다.

다음은 시작 및 종료 값에 대한 검증 규칙입니다.

- 최종 수명이 지정된 경우 시작 수명은 null이 될 수 없습니다.
- 수신 또는 전송 수명의 시작 수명은 종료 수명보다 이전이어야 합니다.

단계 **10** **Add(**추가**)**를 클릭합니다.

키를 생성하려면 5~10단계를 반복합니다. 키 체인에 수명이 중복되는 키를 최소 2개 생성합니다. 이렇게 하면 액티브 키가 없기 때문에 키 보안 통신이 손실되는 것을 방지하는 데 도움이 됩니다.

단계 **11** 개체에 대한 재정의를 관리합니다.

- 이 개체에 대한 재정의를 허용하려면 **Allow Overrides(**재정의 허용**)** 확인란을 선택합니다. 개체 재정의 허용, 13 페이지의 내용을 참조하십시오.
- 이 개체에 재정의 값을 추가하려면 Override(재정의) 섹션을 펼치고 **Add(**추가**)**를 클릭합니다. 개체 재정의 추가, 14 페이지의 내용을 참조하십시오.

단계 **12** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

- 활성 정책이 개체를 참조하는 경우 구성 변경 사항을 구축합니다. 참조.

네트워크

네트워크 개체는 하나 이상의 IP 주소를 나타냅니다. 액세스 제어 정책, 네트워크 변수, ID 규칙, 네트워크 검색 규칙, 이벤트 검색, 보고서, ID 정책 등 여러 위치에서 네트워크 개체 및 그룹을 사용할 수 있습니다.

네트워크 개체가 필요한 옵션을 구성할 경우, 목록은 해당 옵션에 유효한 개체만 표시하도록 자동으로 필터링됩니다. 예를 들어 일부 옵션에는 호스트 개체가 필요하지만 다른 옵션에는 서브넷이 필요합니다.

네트워크 개체는 다음 유형 중 하나일 수 있습니다.

호스트

단일 IP 주소입니다.

IPv4 예:

```
209.165.200.225
```

IPv6 예:

`2001:DB8::0DB8:800:200C:417A` 또는 `2001:DB8:0:0:0DB8:800:200C:417A`

범위

IP 주소의 범위입니다.

IPv4 예:

```
209.165.200.225-209.165.200.250
```

IPv6 예:

```
2001:db8:0:cd30::1-2001:db8:0:cd30::1000
```

네트워크

주소 블록, 또는 서브넷이라고도 합니다.

IPv4 예:

```
209.165.200.224/27
```

IPv6 예:

```
2001:DB8:0:CD30::/60
```

참고 보안 인텔리전스는 `/0` 넷마스크를 사용하는 IP 주소 차단을 무시합니다.

FQDN

단일 FQDN(Fully-Qualified Domain Name) FQDN 확인을 IPv4 주소 전용, IPv6 주소 전용 또는 IPv4 및 IPv6 주소 모두로 제한할 수 있습니다. FQDN은 숫자 또는 문자로 시작하고 끝나야 합니다. FQDN의 처음과 시작을 제외한 위치에는 문자, 숫자, 하이픈만 사용할 수 있습니다.

예를 들면 다음과 같습니다.

```
www.example.com
```

참고 FQDN 개체는 액세스 제어 규칙과 사전 필터링 규칙 또는 수동 NAT 규칙에서만 사용할 수 있습니다. 규칙은 DNS 조회를 통해 FQDN에서 획득한 IP 주소와 일치 여부를 확인합니다. FQDN 네트워크 개체를 사용하려면 DNS 서버 그룹, 32 페이지의 DNS 서버 설정과 DNS 구성의 DNS 플랫폼 설정을 구성했는지 확인해야 합니다.

ID 규칙에서 FDQN 네트워크 개체를 사용할 수 없습니다.

그룹

네트워크 개체의 그룹 또는 기타 네트워크 개체 그룹입니다. 네트워크 개체 그룹을 다른 네트워크 개체 그룹에 추가하여 중첩된 그룹을 생성할 수 있습니다. 최대 10개 수준의 그룹을 중첩할 수 있습니다.

네트워크 와일드카드 마스크

Object Management(개체 관리) 페이지에서 와일드카드 마스크 개체를 생성하고 관리할 수 있습니다.

확장된 서브넷 IP 주소를 사용하여 네트워크 개체를 생성할 수 있습니다. 기존 네트워크 개체는 네트워크 및 네트워크 와일드카드 개체를 모두 지원하도록 확장됩니다. 와일드카드 마스크를 사용하는 네트워크 개체는 네트워크 개체 목록 페이지의 **Type(**유형**)** 열에 **Network Wildcard(**네트워크 와일드카드**)**로 나열됩니다.

와일드카드 마스크는 불연속 비트 마스크인 IP 주소입니다. 연속 마스크를 사용하여 표준 네트워크 개체 및 와일드카드 네트워크 개체에 대한 불연속 마스크를 생성할 수 있습니다.

IP 주소 예	네트워크 와일드카드**?**	개체 유형
192.0.0.0/8	아니요	네트워크
10.10.0.0/255.255.0.0	아니요	네트워크
10.10.0.10/255.255.0.255	예	네트워크 와일드카드
72.0.240.10/255.255.240.255	예	네트워크 와일드카드

참고 네트워크 와일드카드 개체 및 네트워크 와일드카드 개체를 포함하는 개체 그룹은 다음 정책을 구성하는 동안에만 허용됩니다.

- 사전 필터 정책
- 액세스 제어 정책
- NAT 정책

지침 및 제한 사항

- 네트워크 와일드카드 개체를 생성하려면 FMC UI에서 **Objects(**개체**)** > **Object Management(**개체 관리**)** > **Network(**네트워크**)**를 선택하고 **Add Network(**네트워크 추가**)**, **Add Object(**개체 추가**)**를 차례로 클릭합니다. **Network(**네트워크**)** 옵션을 선택하고 값을 확장된 서브넷 마스크로 입력합니다. 예: 10.0.10.10/255.255.0.255.
- 개체 재정의, 그룹 개체 지원, 그룹 개체 재정의, 와일드카드 리터럴 및 와일드카드 개체 가져오기가 지원됩니다.
- 네트워크 와일드카드 개체는 IPv4 주소에 대해서만 지원됩니다.
- 네트워크 와일드카드 개체는 FMC 및 FTD 7.1 버전부터 지원됩니다.
- 네트워크 와일드카드 개체는 Snort-3에 대해서만 지원됩니다.

네트워크 개체 생성

Threat DefenseFeature History(기능 기록**):**

프로시저

단계 **1** **Objects(**개체**)** > **Object Management(**개체 관리**)**을(를) 선택합니다.

단계 **2** 개체 유형 목록에서 **Network(**네트워크**)**를 선택합니다.

단계 **3** **Add Network(**네트워크 추가**)** 드롭다운 메뉴에서 **Add Object(**개체 추가**)**를 선택합니다.

단계 **4** **Name(**이름**)**을 입력합니다.

다중 도메인 구축에서 개체 이름은 도메인 계층 내에서 고유해야 합니다. 시스템은 현재 도메인에서 확인할 수 없는 개체 이름과의 충돌을 식별할 수 있습니다.

단계 **5** 필요한 경우 **Description(**설명**)**을 입력합니다.

단계 **6** **Network(**네트워크**)** 필드에서 필요한 옵션을 선택하고 적절한 값을 입력하려면 네트워크, 45 페이지를 참조합니다.

단계 **7** (FQDN 개체 한정) FQDN과 관련된 IPv4, IPv6 또는 IPv4 및 IPv6 주소를 선택해 사용하려면 **Lookup(**검색**)** 드롭다운 메뉴에서 DNS 확인을 선택합니다.

단계 **8** 개체에 대한 재정의를 관리합니다.

- 이 개체에 대한 재정의를 허용하려면 **Allow Overrides(**재정의 허용**)** 확인란을 선택합니다. 개체 재정의 허용, 13 페이지의 내용을 참조하십시오.
- 이 개체에 재정의 값을 추가하려면 Override(재정의) 섹션을 펼치고 **Add(**추가**)**를 클릭합니다. 개체 재정의 추가, 14 페이지의 내용을 참조하십시오.

단계 **9** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

- 활성 정책이 개체를 참조하는 경우 구성 변경 사항을 구축합니다. 참조.

네트워크 개체 가져오기

네트워크 개체 가져오기에 대한 자세한 내용은 개체 가져오기, 5 페이지의 내용을 참조하십시오.

PKI

SSL 애플리케이션에 대한 **PKI** 개체

PKI 개체는 구축을 지원하는 데 필요한 공개 키 인증서 및 페어링된 개인 키를 나타냅니다. 내부 및 신뢰받는 CA 개체는 CA(인증 기관) 인증서로 구성되며, 내부 CA 개체는 인증서와 페어링된 개인 키도 포함합니다. 내부 및 외부 인증서 개체는 서버 인증서로 구성되며, 내부 인증서 개체는 인증서와 페어링된 개인 키도 포함합니다.

신뢰할 수 있는 인증 기관 개체 및 내부 인증 개체를 사용해 ISE/ISE-PIC에 대한 연결을 설정하는 경우 ISE/ISE-PIC를 ID 소스로 사용할 수 있습니다.

내부 인증 개체를 사용해 캡티브 포털을 설정하는 경우 시스템은 사용자의 웹 드라우저에 연결할 때 캡티브 포털 디바이스의 ID를 인증할 수 있습니다.

신뢰할 수 있는 인증 기관 개체를 사용해 영역을 구성하는 경우 LDAP 또는 AD 서버에 보안 연결을 구성할 수 있습니다.

SSL 규칙에서 PKI 개체를 사용하는 경우 다음을 사용해 암호화된 트래픽을 일치시킬 수 있습니다.

- 외부 인증서 개체의 인증서
- 신뢰받는 CA 개체에서 또는 CA의 신뢰 체인 내에서 CA에 의해 서명된 인증서

SSL 규칙에서 PKI 개체를 사용하는 경우 다음을 사용해 암호 해독을 할 수 있습니다.

- 발신 트래픽 - 내부 CA 개체로 서버 인증서를 다시 서명
- 수신 트래픽 - 내부 인증서 개체에서 알려진 개인 키를 사용하여

인증서와 키 정보를 수동으로 입력하거나, 해당 정보를 포함하는 파일을 업로드하거나, 경우에 따라 새 CA 인증서와 개인 키를 생성할 수 있습니다.

개체 관리자에서 PKI 개체의 목록을 볼 때 인증서의 주체 DN이 개체 값으로서 표시됩니다. 전체 인증서 주체 DN을 보려면 값 위로 포인터를 이동하십시오. 다른 인증서 세부사항을 보려면 PKI 개체를 수정하십시오.

참고 management center 및 관리되는 디바이스는 저장하기 전에 무작위로 생성된 키를 이용하여 내부 CA 개체 및 내부 인증서 개체에 저장된 모든 개인 키를 암호화합니다. 비밀번호로 보호된 개인 키를 업로드하면 어플라이언스는 사용자 제공 비밀번호를 사용해 키를 암호 해독한 다음 저장 전에 무작위로 생성된 키를 사용하여 다시 암호화합니다.

인증서 등록을 위한 **PKI** 개체

인증서 등록 개체에는 CSR(Certificate Signing Requests)을 생성하고 지정된 CA(Certification Authority)에서 ID 인증서를 가져오기 위해 필요한 CA 서버 정보 및 등록 파라미터가 포함되어 있습니다. 이러한 활동은 PKI(Private Key Infrastructure)에서 발생합니다.

인증서 등록 개체에는 인증서 해지 정보도 포함될 수 있습니다. PKI, 디지털 인증서, 인증서 등록에 대한 자세한 내용은 PKI 인프라 및 디지털 인증서을 참조하십시오.

내부 인증 기관 개체

사용자가 구성하는 각 내부 CA(인증 기관) 개체는 조직에서 제어하는 CA의 CA 공개 키 인증서를 나타냅니다. 개체는 개체 이름, CA 인증서 및 페어링된 개인 키로 구성됩니다. SSL 규칙의 내부 CA 개체 및 그룹을 사용해 내부 CA로 서버 인증서를 다시 서명하면 암호화된 발신 트래픽을 암호 해독할 수 있습니다.

참고 **Decrypt - Resign(**암호 해독 - 다시 서명**)** SSL 규칙에서 내부 CA 개체를 참조하고 규칙이 암호화된 세션과 일치하는 경우, 사용자의 브라우저에 SSL 핸드셰이크를 협상하는 동안 인증서가 신뢰되지 않는다는 경고 메시지가 표시될 수 있습니다. 이 문제를 피하려면 내부 CA 개체 인증서를 신뢰받는 루트 인증서의 클라이언트 또는 도메인 목록에 추가하십시오.

다음과 같은 방법으로 내부 CA 개체를 생성할 수 있습니다.

- 기존의 RSA 기반 또는 EC(Elliptic Curve) 기반 CA 인증서와 개인 키 가져오기
- 새로운 자체 서명 RSA 기반 CA 인증서 및 개인 키 생성
- 서명되지 않은 RSA 기반 CA 인증서 및 개인 키 생성 내부 CA 개체를 사용하려면 우선 인증서 서명을 위해 CSR(certificate signing request)을 다른 CA에 제출해야 합니다.

서명된 인증서를 포함하는 내부 CA 개체를 생성한 후에 CA 인증서 및 개인 키를 다운로드할 수 있습니다. 시스템은 다운로드된 인증서 및 개인 키를 사용자 제공 비밀번호로 암호화합니다.

시스템 또는 사용자 생성 여부와 관계없이 내부 CA 개체 이름은 수정할 수 있지만 다른 개체 속성은 수정할 수 없습니다.

사용 중인 내부 CA 개체는 삭제할 수 없습니다. 또한 SSL 정책에서 사용되는 내부 CA 개체를 편집하면 관련 액세스 제어 정책이 오래된 상태가 됩니다. 변경 사항을 적용하려면 액세스 제어 정책을 재구축해야 합니다.

CA 인증서 및 개인 키 가져오기

X.509 v3 CA 인증서 및 개인 키를 가져와서 내부 CA 개체를 구성할 수 있습니다. 다음의 지원되는 형식 중 하나로 인코딩된 파일을 업로드할 수 있습니다.

- DER(Distinguished Encoding Rules)
- PEM(Privacy-enhanced Electronic Mail)

개인 키 파일이 비밀번호로 보호되는 경우 암호 해독 비밀번호를 제공할 수 있습니다. 인증서와 키가 PEM 형식으로 인코딩된 경우 정보를 복사하여 붙여넣을 수도 있습니다.

적절한 인증서 또는 키 정보를 포함하며 상호 페어링된 파일만 업로드할 수 있습니다. 시스템은 개체를 저장하기 전에 페어링을 검증합니다.

참고 **Decrypt - Resign(**암호 해독 **-** 다시 서명**)** 작업으로 규칙을 구성할 경우 이 규칙은 구성된 규칙 조건과 더불어 참조된 내부 CA 인증서의 인증 알고리즘 유형을 기반으로 트래픽을 매칭합니다. 예를 들어 EC(Elliptic Curve) 기반 알고리즘으로 암호화된 발신 트래픽을 암호 해독 하려면 EC 기반 CA 인증서를 업로드해야 합니다.

CA 인증서 및 개인 키 가져오기

다중 도메인 구축에서 시스템은 현재 도메인에서 생성된 개체를 표시하며 이러한 개체는 수정할 수 있습니다. 상위 도메인에서 생성된 개체도 표시되지만, 이러한 개체는 수정할 수 없습니다. 하위 도메인에서 생성된 개체를 보고 수정하려면 해당 도메인으로 전환하십시오.

프로시저

단계 **1** **Objects(**개체**)** > **Object Management(**개체 관리**)**을(를) 선택합니다.

단계 **2** **PKI** 노드를 확장하고 내부 **CA**를 선택합니다.

단계 **3** **Import CA**를 클릭합니다.

단계 **4** **Name(**이름**)**을 입력합니다.

다중 도메인 구축에서 개체 이름은 도메인 계층 내에서 고유해야 합니다. 시스템은 현재 도메인에서 확인할 수 없는 개체 이름과의 충돌을 식별할 수 있습니다.

단계 **5** **Certificate Data** 필드 위에서 **Browse**를 클릭하여 DER 또는 PEM으로 인코딩된 X.509 v3 CA 인증서 파일을 업로드합니다.

단계 **6** **Key** 필드 위에서 **Browse**를 클릭하여 DER 또는 PEM으로 인코딩된 페어링된 개인 키 파일을 업로드합니다.

단계 **7** 업로드 파일이 비밀번호로 보호된 경우 **Encrypted, and the password is:(**암호화됨**,** 비밀번호**:)** 체크 박스를 선택하고 비밀번호를 입력합니다.

단계 **8** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

- 활성 정책이 개체를 참조하는 경우 구성 변경 사항을 구축합니다. 참조.

새 **CA** 인증서 및 개인 키 생성

자체 서명 RSA 기반 CA 인증서 및 개인 키를 생성하기 위한 식별 정보를 제공하여 내부 CA 개체를 구성할 수 있습니다.

생성된 CA 인증서는 10년간 유효합니다. Valid From 날짜는 생성 이전의 주입니다.

다중 도메인 구축에서 시스템은 현재 도메인에서 생성된 개체를 표시하며 이러한 개체는 수정할 수 있습니다. 상위 도메인에서 생성된 개체도 표시되지만, 이러한 개체는 수정할 수 없습니다. 하위 도메인에서 생성된 개체를 보고 수정하려면 해당 도메인으로 전환하십시오.

프로시저

단계 **1** **Objects(**개체**)** > **Object Management(**개체 관리**)**을(를) 선택합니다.

단계 **2** **PKI** 노드를 확장하고 내부 **CA**를 선택합니다.

단계 **3** **Generate CA(CA** 생성**)**를 클릭하고

단계 **4** **Name(**이름**)**을 입력합니다.

다중 도메인 구축에서 개체 이름은 도메인 계층 내에서 고유해야 합니다. 시스템은 현재 도메인에서 확인할 수 없는 개체 이름과의 충돌을 식별할 수 있습니다.

단계 **5** 식별 속성을 입력합니다.

단계 **6** **Generate self-signed CA(**자체 서명된 **CA** 생성**)**를 클릭합니다.

새로 서명된 인증서

CA에서 서명된 인증서를 가져와서 내부 CA 개체를 구성할 수 있습니다. 여기에는 두 단계가 관련됩니다.

- 내부 CA 개체를 구성하기 위한 식별 정보를 제공합니다. 그러면 서명되지 않은 인증서와 페어링된 개인 키, 그리고 사용자가 지정한 CA에 대한 CSR(certificate signing request)이 생성됩니다.
- CA가 서명된 인증서를 발행하면 이를 내부 CA 개체에 업로드하여 서명되지 않은 인증서를 교체합니다.

SSL 규칙에서 내부 CA 개체만 참조할 수 있습니다(해당 개체에 서명된 인증서가 포함된 경우).

서명되지 않은 CA 인증서 및 CSR 생성

프로시저

단계 1 **Objects(**개체**)** > **Object Management(**개체 관리**)**을(를) 선택합니다.

단계 2 **PKI** 노드를 확장하고 내부 **CA**를 선택합니다.

단계 3 **Generate CA(CA** 생성**)**를 클릭하고

단계 4 **Name(**이름**)**을 입력합니다.

다중 도메인 구축에서 개체 이름은 도메인 계층 내에서 고유해야 합니다. 시스템은 현재 도메인에서 확인할 수 없는 개체 이름과의 충돌을 식별할 수 있습니다.

단계 5 식별 속성을 입력합니다.

단계 6 **Generate CSR**을 클릭합니다.

단계 7 CA에 제출할 CSR을 복사합니다.

단계 8 **OK(**확인**)**를 클릭합니다.

다음에 수행할 작업

- 에 설명된 대로 CA에서 발급한 서명된 인증서를 업로드해야 합니다. CSR에 응답하여 발행된 서명된 인증서 업로드, 52 페이지

CSR에 응답하여 발행된 서명된 인증서 업로드

다중 도메인 구축에서 시스템은 현재 도메인에서 생성된 개체를 표시하며 이러한 개체는 수정할 수 있습니다. 상위 도메인에서 생성된 개체도 표시되지만, 이러한 개체는 수정할 수 없습니다. 하위 도메인에서 생성된 개체를 보고 수정하려면 해당 도메인으로 전환하십시오.

업로드가 끝나면 SSL 규칙에서 서명된 인증서를 참조할 수 있습니다.

프로시저

단계 1 **Objects(**개체**)** > **Object Management(**개체 관리**)**을(를) 선택합니다.

단계 2 **PKI** 노드를 확장하고 내부 **CA**를 선택합니다.

단계 3 CSR을 기다리는 서명되지 않은 인증서가 포함된 CA 개체 옆에 있는 **Edit(**수정**)** ( )을 클릭합니다.

단계 4 **Install Certificate(**인증서 설치**)**를 클릭합니다.

단계 5 DER 또는 PEM으로 인코딩된 X.509 v3 CA 인증서 파일을 업로드하려면 **Browse(**찾아보기**)**를 클릭합니다.

단계 6 업로드된 파일이 비밀번호로 보호된 경우 **Encrypted, and the password is:(**암호화됨**,** 비밀번호**:)** 체크 박스를 선택하고 비밀번호를 입력합니다.

단계 **7** CA 개체에 서명된 인증서를 업로드하려면 **Save(**저장**)**을 클릭합니다.

다음에 수행할 작업

- 활성 정책이 개체를 참조하는 경우 구성 변경 사항을 구축합니다. 참조.

CA 인증서 및 개인 키 다운로드

내부 CA 개체의 인증서 및 키 정보를 포함하는 파일을 다운로드하여 CA 인증서 및 페어링된 개인 키를 백업하거나 전송할 수 있습니다.

주의 다운로드한 키 정보는 항상 안전한 장소에 저장하십시오.

시스템은 내부 CA 개체에 저장된 개인 키를 무작위로 생성된 키로 암호화한 후 디스크에 저장합니다. 내부 CA 개체에서 인증서와 개인 키를 다운로드하면 시스템은 인증서 및 개인 키 정보를 포함하는 파일을 생성하기 전에 먼저 해당 정보를 해독합니다. 그런 다음 시스템이 다운로드한 파일을 암호화하는 데 사용할 비밀번호를 제공해야 합니다.

주의 시스템 백업 과정에서 다운로드된 개인 키는 해독된 후 암호화되지 않은 백업 파일에 저장됩니다.

CA 인증서 및 개인 키 다운로드

다중 도메인 구축에서 시스템은 현재 도메인에서 생성된 개체를 표시하며 이러한 개체는 수정할 수 있습니다. 상위 도메인에서 생성된 개체도 표시되지만, 이러한 개체는 수정할 수 없습니다. 하위 도메인에서 생성된 개체를 보고 수정하려면 해당 도메인으로 전환하십시오.

현재 도메인 및 상위 도메인에 대한 CA 인증서를 다운로드할 수 있습니다.

프로시저

단계 **1** **Objects(**개체**)** > **Object Management(**개체 관리**)**을(를) 선택합니다.

단계 **2** **PKI** 노드를 확장하고 내부 **CA**를 선택합니다.

단계 **3** 다운로드할 인증서 및 개인 키에 해당하는 내부 CA 개체 옆의 **Edit(**수정**)** ( )을 클릭합니다.

다중 도메인 구축의 경우, **View(**보기**)** ( )을 클릭하면 상위 도메인의 개체에 대한 인증서 및 개인 키를 다운로드할 수 있습니다.

단계 **4** **Download(**다운로드**)**를 클릭합니다.

단계 **5** **Password(**비밀번호**)** 및 **Confirm Password(**비밀번호 확인**)** 필드에 암호화 비밀번호를 입력합니다.

단계 **6** **OK(**확인**)**를 클릭합니다.

신뢰할 수 있는 인증 기관 개체

사용자가 구성하는 신뢰받는 인증 기관(CA) 개체는 신뢰받는 CA에 속한 CA 공개 키 인증서를 나타냅니다. 개체는 개체 이름 및 CA 공개 키 인증서로 구성됩니다. 다음의 경우에 외부 CA 개체 및 그룹을 사용할 수 있습니다.

- 트래픽을 제어하기 위한 SSL 정책이 신뢰받는 CA 또는 신뢰 체인의 CA가 서명한 인증서로 암호화된 경우
- LDAP 또는 AD 서버에 보안 연결을 설정하기 위한 영역 설정
- ISE/ISE-PIC 연결 **pxGrid** 서버 **CA** 및 **MNT** 서버 **CA** 필드에 대해 신뢰받는 인증 기관 개체를 선택합니다.

신뢰받는 CA 개체를 생성한 후에는 이름을 수정하고 CRL(certificate revocation lists)을 추가할 수 있지만 다른 개체 속성은 수정할 수 없습니다. 개체에 추가할 수 있는 CRL의 수에는 제한이 없습니다. 개체에 업로드한 CRL을 수정하려면 개체를 삭제하고 다시 생성해야 합니다.

참고 개체가 ISE/ISE-PIC 통합 설정에서 사용될 경우 개체에 CRL을 추가하는 것은 효과가 없습니다.

사용 중인 신뢰받는 CA 개체는 삭제할 수 없습니다. 또한 사용되는 신뢰받는 CA 개체를 편집하면 관련 액세스 제어 정책이 오래된 상태가 됩니다. 변경 사항을 적용하려면 액세스 제어 정책을 재구축해야 합니다.

신뢰할 수 있는 **CA** 개체

X.509 v3 CA 인증서를 업로드하여 외부 CA 개체를 구성할 수 있습니다. 다음의 지원되는 형식 중 하나로 인코딩된 파일을 업로드할 수 있습니다.

- DER(Distinguished Encoding Rules)
- PEM(Privacy-enhanced Electronic Mail)

파일이 비밀번호로 보호된 경우 암호 해독 비밀번호를 제공해야 합니다. 인증서가 PEM 형식으로 인코딩된 경우 정보를 복사하여 붙여넣을 수도 있습니다.

파일에 적절한 인증서 정보가 포함된 경우에만 CA 인증서를 업로드할 수 있습니다. 시스템은 개체를 저장하기 전에 인증서를 검증합니다.

신뢰할 수 있는 **CA** 개체 추가

프로시저

단계 **1** **Objects(**개체**)** > **Object Management(**개체 관리**)**을(를) 선택합니다.

단계 **2** **PKI** 노드를 확장하고 신뢰받는 **CA**를 선택합니다.

단계 **3** **Add Trusted CAs**를 클릭합니다.

단계 **4** **Name(**이름**)**을 입력합니다.

다중 도메인 구축에서 개체 이름은 도메인 계층 내에서 고유해야 합니다. 시스템은 현재 도메인에서 확인할 수 없는 개체 이름과의 충돌을 식별할 수 있습니다.

단계 **5** DER 또는 PEM으로 인코딩된 X.509 v3 CA 인증서 파일을 업로드하려면 **Browse(**찾아보기**)**를 클릭합니다.

단계 **6** 파일이 비밀번호로 보호된 경우 **Encrypted, and the password is:(**암호화됨**,** 비밀번호**:)** 체크 박스를 선택하고 비밀번호를 입력합니다.

단계 **7** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

- 활성 정책이 개체를 참조하는 경우 구성 변경 사항을 구축합니다. 참조.

신뢰할 수 있는 **CA** 개체의 인증서 해지 목록

CRL을 신뢰받는 CA 개체에 업로드할 수 있습니다. SSL 정책에서 해당 신뢰받는 CA 개체를 참조하는 경우, 세션 암호화 인증서를 발행한 CA가 그 이후 인증서를 폐기했는지 여부에 따라 암호화된 트래픽을 제어할 수 있습니다. 다음의 지원되는 형식 중 하나로 인코딩된 파일을 업로드할 수 있습니다.

- DER(Distinguished Encoding Rules)
- PEM(Privacy-enhanced Electronic Mail)

CRL을 추가한 후에는 폐기된 인증서의 목록을 볼 수 있습니다. 개체에 업로드한 CRL을 수정하려면 개체를 삭제하고 다시 생성해야 합니다.

적절한 CRL을 포함하는 파일만 업로드할 수 있습니다. 신뢰받는 CA 개체에 추가할 수 있는 CRL의 수에는 제한이 없습니다. 그러나 CRL을 업로드할 때마다 또 다른 CRL을 추가하기 전에 개체를 저장해야 합니다.

참고 개체가 ISE/ISE-PIC 통합 설정에서 사용될 경우 개체에 CRL을 추가하는 것은 효과가 없습니다.

신뢰할 수 있는 **CA** 개체에 인증서 해지 목록 추가

다중 도메인 구축에서 시스템은 현재 도메인에서 생성된 개체를 표시하며 이러한 개체는 수정할 수 있습니다. 상위 도메인에서 생성된 개체도 표시되지만, 이러한 개체는 수정할 수 없습니다. 하위 도메인에서 생성된 개체를 보고 수정하려면 해당 도메인으로 전환하십시오.

참고 개체가 ISE/ISE-PIC 통합 설정에서 사용될 경우 개체에 CRL을 추가하는 것은 효과가 없습니다.

프로시저

단계 **1** **Objects(**개체**)** > **Object Management(**개체 관리**)**을(를) 선택합니다.

단계 **2** **PKI** 노드를 확장하고 신뢰받는 **CA**를 선택합니다.

단계 **3** 신뢰받는 CA 개체 옆에 있는 **Edit(**수정**)** ( )을 클릭합니다.

View(보기**)** ( )이 대신 표시되는 경우에는 설정이 상위 도메인에 속하거나 설정을 수정할 권한이 없는 것입니다.

단계 **4** DER 또는 PEM으로 인코딩된 CRL 파일을 업로드하려면 **Add CRL(CRL** 추가**)**를 클릭합니다.

단계 **5** **OK(**확인**)**를 클릭합니다.

다음에 수행할 작업

- 활성 정책이 개체를 참조하는 경우 구성 변경 사항을 구축합니다. 참조.

외부 인증서 개체

사용자가 구성하는 각 외부 인증서 개체는 조직에 속하지 않은 서버 공개 키 인증서를 나타냅니다. 개체는 개체 이름 및 인증서로 구성됩니다. 서버 인증서로 암호화된 트래픽을 제어하려면 SSL 규칙에서 외부 인증서 개체 및 그룹을 사용할 수 있습니다. 예를 들어 사용자는 신뢰하는 자체 서명 서버 인증서를 업로드할 수는 있지만 신뢰할 수 있는 CA 인증서로 확인할 수는 없습니다.

X.509 v3 서버 인증서를 업로드하여 외부 인증서 개체를 구성할 수 있습니다. 다음의 지원되는 형식 중 하나로 파일을 업로드할 수 있습니다.

- DER(Distinguished Encoding Rules)
- PEM(Privacy-enhanced Electronic Mail)

적절한 서버 인증서 정보가 포함된 파일만 업로드할 수 있습니다. 시스템은 개체를 저장하기 전에 파일을 검증합니다. 인증서가 PEM 형식으로 인코딩된 경우 정보를 복사하여 붙여넣을 수도 있습니다.

외부 인증서 개체 추가

프로시저

단계 **1** **Objects(**개체**)** > **Object Management(**개체 관리**)**을(를) 선택합니다.

단계 **2** **PKI** 노드를 확장하고 외부 인증서를 선택합니다.

단계 **3** **Add External Cert**를 클릭합니다.

단계 **4** **Name(**이름**)**을 입력합니다.

다중 도메인 구축에서 개체 이름은 도메인 계층 내에서 고유해야 합니다. 시스템은 현재 도메인에서 확인할 수 없는 개체 이름과의 충돌을 식별할 수 있습니다.

단계 **5** **Certificate Data(**인증서 데이터**)** 필드 위에서 **Browse(**찾아보기**)**를 클릭하여 DER 또는 PEM으로 인코딩된 X.509 v3 서버 인증서 파일을 업로드합니다.

단계 **6** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

- 활성 정책이 개체를 참조하는 경우 구성 변경 사항을 구축합니다. 참조.

내부 인증서 개체

사용자가 구성하는 각 내부 인증서 개체는 조직에 속한 서버 공개 키 인증서를 나타냅니다. 개체는 개체 이름, 공개 키 인증서 및 페어링된 개인 키로 구성됩니다. 다음의 경우 내부 인증서 개체 및 그룹을 사용할 수 있습니다.

- 알려진 개인 키를 사용하여 조직의 서버 중 하나로 들어오는 트래픽을 해독하려는 SSL 규칙
- ISE/ISE-PIC 연결 **MC** 서버 인증서 필드에 내부 인증서 개체를 선택합니다.
- 사용자의 웹 브라우저에 연결할 때 캡티브 포털 디바이스의 ID를 인증하는 캡티브 포털 설정 서버 인증서 필드에 내부 인증서 개체를 선택합니다.

X.509 v3 RSA 기반 또는 EC(Elliptic Curve) 기반 서버 인증서 및 페어링된 개인 키를 업로드하여 내부 인증서 개체를 구성할 수 있습니다. 다음의 지원되는 형식 중 하나로 파일을 업로드할 수 있습니다.

- DER(Distinguished Encoding Rules)
- PEM(Privacy-enhanced Electronic Mail)

파일이 비밀번호로 보호된 경우 암호 해독 비밀번호를 제공해야 합니다. 인증서와 키가 PEM 형식으로 인코딩된 경우 정보를 복사하여 붙여넣을 수도 있습니다.

적절한 인증서 또는 키 정보를 포함하며 상호 페어링된 파일만 업로드할 수 있습니다. 시스템은 개체를 저장하기 전에 페어링을 검증합니다.

내부 인증서 개체를 생성한 후에는 이름을 수정할 수 있지만 다른 개체 속성은 수정할 수 없습니다.

사용 중인 내부 인증서 개체는 삭제할 수 없습니다. 또한 사용 중인 내부 인증서 개체를 편집하면 관련 액세스 제어 정책이 오래된 상태가 됩니다. 변경 사항을 적용하려면 액세스 제어 정책을 재구축해야 합니다.

내부 인증서 개체 추가

프로시저

단계 **1** **Objects(**개체**)** > **Object Management(**개체 관리**)**을(를) 선택합니다.

단계 **2** **PKI** 노드를 확장하고 내부 인증서를 선택합니다.

단계 **3** **Add Internal Cert**를 클릭합니다.

단계 **4** **Name(**이름**)**을 입력합니다.

다중 도메인 구축에서 개체 이름은 도메인 계층 내에서 고유해야 합니다. 시스템은 현재 도메인에서 확인할 수 없는 개체 이름과의 충돌을 식별할 수 있습니다.

단계 **5** **Certificate Data(**인증서 데이터**)** 필드 위에서 **Browse(**찾아보기**)**를 클릭하여 DER 또는 PEM으로 인코딩된 X.509 v3 서버 인증서 파일을 업로드합니다.

단계 **6** **Key** 필드 위에서 **Browse**를 클릭하여 DER 또는 PEM으로 인코딩된 페어링된 개인 키 파일을 업로드합니다.

단계 **7** 업로드된 개인 키 파일이 비밀번호로 보호된 경우 **Encrypted, and the password is:(**암호화됨**,** 비밀번호**:)** 체크 박스를 선택하고 비밀번호를 입력합니다.

단계 **8** **Save(**저장**)**를 클릭합니다.

인증서 등록 개체

신뢰 지점을 사용하여 CA와 인증서를 관리하고 추적할 수 있습니다. 신뢰 지점은 CA 또는 ID 쌍을 나타낸 것입니다. 신뢰 지점에는 CA의 ID, CA별 구성 파라미터, 하나의 등록된 ID 인증서와의 연결 관계가 포함되어 있습니다.

인증서 등록 개체에는 CSR(Certificate Signing Requests)을 생성하고 지정된 CA(Certification Authority)에서 ID 인증서를 가져오기 위해 필요한 CA 서버 정보 및 등록 파라미터가 포함되어 있습니다. 이러한 활동은 PKI(Private Key Infrastructure)에서 발생합니다.

인증서 등록 개체에는 인증서 해지 정보도 포함될 수 있습니다. PKI, 디지털 인증서, 인증서 등록에 대한 자세한 내용은 PKI 인프라 및 디지털 인증서을 참조하십시오.

인증서 등록 개체의 사용 방법

인증서 등록 개체는 PKI 인프라에 관리되는 디바이스를 등록하고 다음을 통해 VPN 연결을 지원하는 디바이스에 트러스트 포인트(CA 개체)를 생성합니다.

1. CA 인증 및 인증서 등록 개체 등록에 대한 파라미터를 정의합니다. 공유 파라미터를 지정하고 다른 디바이스에 대해 고유한 개체 설정을 지정하기 위해 오버라이드 기능을 사용합니다.
2. ID 인증서를 요구하는 관리되는 각 디바이스에 개체를 설치 및 연결합니다. 디바이스에서 이는 트러스트 포인트가 됩니다.

인증서 등록 개체이 연결된 후 디바이스에 설치되면 인증서 등록 프로세스가 즉시 시작됩니다. 자체 서명, SCEP, EST 및 PKCS12 파일 등록 유형의 경우 이 프로세스는 자동으로 진행되므로, 관리자의 추가 작업이 필요하지 않습니다. 수동 인증서 등록에는 관리자의 추가 작업이 필요합니다.

3. VPN 구성에서 생성된 트러스트 포인트를 지정합니다.

인증서 등록 개체 관리

인증서 등록 개체을 관리하려면 개체 > 개체 관리로 이동하고 탐색창에서 **PKI** > 인증서 등록을 선택합니다. 다음 정보가 표시됩니다.

- 기존 인증서 등록 개체는 **Name(**이름**)** 열에 표시됩니다.

  검색 필드(돋보기)를 사용해 목록을 필터링합니다.

- 각 개체의 등록 유형은 **Type(**유형**)** 열에 표시됩니다. 다음 등록 방법을 사용할 수 있습니다.
  - 자체 서명 - 관리되는 디바이스가 자체 서명된 루트 인증서를 생성합니다.
  - **EST** - CA에서 ID 인증서를 얻기 위해 디바이스에서 보안 전송을 통한 등록을 사용합니다.
  - **SCEP** - (기본) SCEP(Simple Certificate Enrollment Protocol)은 디바이스가 CA로부터 ID 인증서를 가져올 때 사용합니다.
  - 수동 - 관리자가 수동으로 등록 프로세스를 수행합니다.
  - **PKCS12** 파일 - VPN 연결을 지원하는 Firepower Threat Defense 관리 디바이스에 PKCS12 파일을 가져옵니다. PKCS#12, PFX 또는 P12에서 파일은 하나의 암호화된 파일에 서버 인증서, 중간 인증서 및 개인 키를 보관합니다. 암호 해독을 위해 **Passphrase(**암호 문구**)** 값을 입력합니다.

- **Override(**오버라이드**)** 열은 개체가 오버라이드를 허용(녹색 확인 표시) 또는 허용 불가(빨간색 X)하는지 여부를 나타냅니다. 숫자가 표시되는 경우 오버라이드의 수를 나타냅니다.

  VPN 구성의 일부인 각 디바이스에 개체 설정을 사용자 정의하려면 오버라이드 옵션을 사용합니다. 오버라이드는 각 디바이스의 트러스트 포인트 세부 정보를 고유하게 만듭니다. 보통 VPN 구성 시 각 디바이스의 일반 이름 또는 제목이 오버라이드됩니다.

  모든 유형의 개체 오버라이드 절차에 대해서는 개체 재정의, 11 페이지를 참조하십시오.

- 편집 아이콘(연필)을 클릭하여 이전에 생성한 인증서 등록 개체를 **Edit(**편집**)**합니다. 등록 개체가 관리되는 디바이스와 연결되지 않은 경우만 편집할 수 있습니다. 편집에 대한 추가 지침은 인증서 등록 개체을 참조하십시오. 등록이 실패한 개체는 편집할 수 있습니다.

- 삭제 아이콘(휴지통)을 클릭하여 이전에 생성한 인증서 등록 개체를 **Delete(**삭제**)**합니다. 관리되는 디바이스와 연결된 경우 인증서 등록 개체을 삭제할 수 없습니다.

Add Cert Enrollment(인증서 등록 추가**)** 대화 상자를 열고 인증서 등록 개체을 구성하려면 **(+) Add Cert Enrollment(**인증서 등록 추가**)**를 누릅니다. 인증서 등록 개체 추가, 60 페이지를 참조하십시오. 각 관리되는 헤드엔드 디바이스에 인증서를 설치합니다.

관련 항목

자체 서명 등록을 사용한 인증서 설치
EST 등록을 사용한 인증서 설치
SCEP 등록을 사용한 인증서 설치
수동 등록을 사용한 인증서 설치
PKCS12 파일을 사용하여 인증서 설치

인증서 등록 개체 추가

이러한 개체는 threat defense 디바이스와 함께 사용할 수 있습니다. 이 작업을 수행하려면 관리자 또는 네트워크 관리자 권한이 있어야 합니다.

프로시저

단계 **1** **Add Cert Enrollment(**인증서 등록 추가**)** 대화 상자를 엽니다.

- 개체 관리자에서 직접 하려는 경우 개체 > 개체 관리 화면에서 탐색창의 **PKI** > 인증서 등록을 선택하고 인증서 등록 추가를 누릅니다.
- 관리되는 디바이스를 구성하는 도중이라면 장치 > 인증서 화면에서 추가 > 새 인증서 추가를 선택하고 **(+)**를 클릭해 인증서 등록 필드를 엽니다.

단계 **2** 개체의 이름과 필요한 경우 설명을 입력합니다.

등록이 완료되면 이 이름은 연결된 관리되는 디바이스의 트러스트 포인트의 이름이 됩니다.

단계 **3** **CA Information(CA** 정보**)** 탭을 열고 **Enrollment Type(**등록 유형**)**을 선택합니다.

- 자체 서명 - 관리되는 디바이스가 CA가 되어 자체 서명된 루트 인증서를 생성합니다. 이 창에서는 기타 정보가 필요하지 않습니다.

  참고 자체 서명 인증서를 등록할 경우 인증서 파라미터에서 CN(Common Name)을 지정해야 합니다.

- **EST**—보안 전송 프로토콜을 통한 등록 EST 정보를 지정합니다. 인증서 등록 개체 EST 옵션, 62 페이지를 참조하십시오.
- **SCEP** - (기본) 단순 인증 등록 프로토콜(Simple Certificate Enrollment Protocol) SCEP 정보를 지정합니다. 인증서 등록 개체 SCEP 옵션, 62 페이지의 내용을 참조하십시오.
- 수동
  - **CA Only(CA** 전용**)** - 선택한 CA에서 CA 인증서만 생성하려면 이 체크 박스를 선택합니다. 이 인증서에 대해 ID 인증서가 생성되지 않습니다.

    이 체크 박스를 선택하지 않으면 CA 인증서가 필수가 아닙니다. CA 인증서 없이 CSR을 생성하고 ID 인증서를 얻을 수 있습니다.

  - **CA Certificate(CA** 인증서**)** - CA 인증서 정보를 상자에 붙여 넣습니다. 다른 디바이스에서 복사하여 CA 인증서를 가져올 수도 있습니다.

    CA 인증서 없이 CSR을 생성하도록 선택하는 경우 이 상자를 비워둘 수 있습니다.

- **PKCS12** 파일 - VPN 연결을 지원하는 threat defense 관리 디바이스에 PKCS12 파일을 가져옵니다. PKCS#12 또는 PFX에서 파일은 하나의 암호화된 파일에 서버 인증서, 중간 인증서 및 개인 키를 보관합니다.암호 해독을 위해 **Passphrase(**암호 문구**)** 값을 입력합니다.
- **Skip Check for CA flag in basic constraints of the CA Certificate(CA** 인증서의 기본 제약 조건에서 **CA** 플래그 확인 건너뛰기**)**—트러스트 포인트 인증서에서 기본 제약 조건 확장 및 CA 플래그 검사를 건너 뛰려면 이 체크 박스를 선택합니다.
- **Validation Usage(**검증 사용**)** - VPN 연결 중에 인증서를 검증하는 옵션을 선택합니다.
  - **IPsec Client(IPsec** 클라이언트**)** - 사이트 간 VPN 연결에 대한 IPsec 클라이언트 인증서를 검증합니다.
  - **SSL Client(SSL** 클라이언트**)** - 원격 액세스 VPN 연결을 시도하는 동안 SSL 클라이언트 인증서를 검증합니다.
  - **SSL Server(SSL** 서버**)** - SSL 서버 인증서를 검증하려면 선택합니다(예: Cisco Umbrella 서버 인증서).

단계 **4** (선택 사항) **Certificate Parameters(**인증서 파라미터**)** 탭을 열고 인증서 내용을 지정합니다. 인증서 등록 개체 인증서 매개변수, 63 페이지의 내용을 참조하십시오.

이 정보는 인증서에 저장되고 라우터에서 인증서를 수신하는 측에서 읽을 수 있습니다.

단계 **5** (선택 사항) **Key(**키**)** 탭을 열고 키 정보를 지정합니다. 인증서 등록 개체 키 옵션, 64 페이지의 내용을 참조하십시오.

단계 **6** (선택 사항) **Revocation(**해지**)** 탭을 클릭하고 해지 옵션을 지정합니다. 인증서 등록 개체 폐기 옵션, 66 페이지를 참조하십시오.

단계 **7** 원하는 경우 개체에 대한 오버라이드를 허용합니다. 개체 오버라이드에 대한 전체 설명은 개체 재정의, 11 페이지을 참조하십시오.

다음에 수행할 작업

디바이스에 트러스트 포인트를 생성하려면 등록 개체를 연결 및 설치합니다.

관련 항목

자체 서명 등록을 사용한 인증서 설치
EST 등록을 사용한 인증서 설치
SCEP 등록을 사용한 인증서 설치
수동 등록을 사용한 인증서 설치
PKCS12 파일을 사용하여 인증서 설치

인증서 등록 개체 **EST** 옵션

Secure Firewall Management Center 탐색 경로

Objects(개체**)** > **Object Management(**개체 관리**)**로 이동한 뒤 탐색 창에서**PKI** > **Cert Enrollment(**인증서 등록**)**를 선택합니다. **(+) Add Cert Enrollment(**인증서 등록 추가**)**를 클릭하여 **Add Cert Enrollment(**인증서 등록 추가**)** 대화 상자를 열고 **CA Information(CA** 정보**)** 탭을 선택합니다.

필드

등록 유형 **- EST**로 설정합니다.

참고

- EST 등록 유형은 EdDSA 키를 지원하지 않습니다.
- EST의 인증서 만료시 디바이스를 자동 등록하는 기능은 지원되지 않습니다.

등록 **URL** - 디바이스가 등록을 시도하는 CA 서버의 URL입니다.

*CA_name*이 CA 서버의 호스트 DNS 이름 또는 IP 주소인 **https://CA_name:port** 형태의 HTTP URL을 사용합니다. 포트 번호는 필수입니다.

Username(사용자 이름**)** - CA 서버에 액세스하기 위한 사용자 이름입니다.

Password / Confirm Password(비밀번호 / 비밀번호 확인**)** - CA 서버에 액세스하기 위한 비밀번호입니다.

Fingerprint(핑거프린트**)** - EST를 사용하여 CA 인증서를 검색하는 경우 CA 서버에 핑거프린트를 입력할 수 있습니다. CA 서버 인증서의 신뢰성을 확인하기 위해 핑거프린트를 사용하면 권한이 없는 사용자가 실제 대신 가짜 인증서를 대체하는 것을 방지할 수 있습니다. 16진수 형태로 CA 서버의 핑거프린트를 입력합니다. 입력한 값이 인증서의 핑거프린트와 일치하지 않으면 인증서가 거부됩니다. 서버에 직접 연결하여 CA의 핑거프린트를 가져옵니다.

Source Interface(소스 인터페이스**)** - CA 서버와 상호 작용하는 인터페이스입니다. 기본적으로 진단 인터페이스가 표시됩니다. 데이터 인터페이스를 소스 인터페이스로 구성하려면 해당 보안 영역 또는 인터페이스 그룹 개체를 선택합니다.

Ignore EST Server Certificate Validations(EST 서버 인증서 검증 무시**)** - EST 서버 인증서 검증은 기본적으로 수행됩니다. EST 서버 인증서를 검증하는 FTD를 무시하려면 확인란을 선택합니다.

인증서 등록 개체 **SCEP** 옵션

Secure Firewall Management Center 탐색 경로

개체 > 개체 관리로 이동한 뒤 탐색창에서 **PKI > PKI** 등록을 선택합니다. **PKI** 등록 추가 대화 상자를 열고 **CA** 정보 탭을 선택하려면 **(+) Add PKI Enrollment(PKI** 등록 추가**)**를 누릅니다.

필드

등록 유형 - **SCEP**로 설정합니다.

등록 **URL** - 디바이스가 등록을 시도하는 CA 서버의 URL입니다.

CA_name이 CA 서버의 호스트 DNS 이름 또는 IP 주소인 **`http://CA_name:port`** 형태의 HTTP URL을 사용합니다. 포트 번호는 필수입니다.

참고 SCEP 서버가 hostname/FQDN을 참조하면 FlexConfig 개체를 사용해 DNS 서버를 구성합니다.

CA의 CA cgi-bin 스크립트 위치가 기본(/cgi-bin/pkiclient.exe)이 아닌 경우 URL에 http://CA_name:port/script_location 형태로 비표준 스크립트 위치를 포함해야 하며, 이 때 script_location은 CA 스크립트의 전체 경로입니다.

비밀 번호 검사/확인 - 디바이스의 ID를 검증하도록 CA 서버에서 사용되는 비밀번호입니다. CA 서버에 직접 연결하거나 웹 브라우저에 **`http://URLHostName/certsrv/mscep/mscep.dll`**을 입력하여 비밀번호를 얻을 수 있습니다. 비밀번호는 CA 서버에서 가져온 뒤 60분 동안 유효합니다. 따라서 생성 후 최대한 빨리 비밀번호를 구축하는 것이 중요합니다.

재시도 간격 - 인증 요청 시도 재시도 간격으로 분 단위로 되어 있습니다. 값은 1~60분입니다. 기본값은 1분입니다.

재시도 수 - 첫 번째 요청에 인증서가 발행되지 않은 경우 재시도 횟수입니다. 값은 1~100입니다. 기본값은 10입니다.

CA 인증서 소스 - CA 인증서를 얻는 방법을 지정합니다.

- **SCEP**를 사용해 검색(기본, 지원되는 경우) - CA 서버에서 SCEP(단순 인증서 등록 프로세스)를 사용해 인증서를 검색합니다. SCEP를 사용하려면 디바이스와 CA 서버 간의 연결이 필요합니다. 등록 프로세스를 시작하기 전 디바이스가 CA 서버에 연결되었는지 확인하십시오.

핑거프린트 - SCEP를 사용하여 CA 인증서를 검색하는 경우 CA 서버에 핑거프린트를 입력할 수 있습니다. CA 서버 인증서의 신뢰성을 확인하기 위해 핑거프린트를 사용하면 권한이 없는 사용자가 실제 대신 가짜 인증서를 대체하는 것을 방지할 수 있습니다. 16진수 형태로 CA 서버의 핑거프린트를 입력합니다. 입력한 값이 인증서의 핑거프린트와 일치하지 않으면 인증서가 거부됩니다. 서버에 직접 연결하거나 웹 브라우저에 **`http://<URLHostName>/certsrv/mscep/mscep.dll`**의 주소를 입력하여 CA의 핑거프린트를 얻을 수 있습니다.

인증서 등록 개체 인증서 매개변수

CA 서버에 전송되는 인증서 요청의 추가 정보를 지정합니다. 이 정보는 인증서에 저장되고 라우터에서 인증서를 수신하는 측에서 읽을 수 있습니다.

Secure Firewall Management Center 탐색 경로

개체 > 개체 관리로 이동한 뒤 탐색창에서 **PKI > PKI** 등록을 선택합니다. **PKI** 등록 추가 대화 상자를 열고 **(+) PKI** 등록 추가를 누른 뒤 인증서 파라미터 탭을 누릅니다.

필드

표준 LDAP X.500 형식을 사용해 모든 정보를 입력합니다.

- **FQDN** 포함 - 인증서 요청에 FQDN(Fully Qualified Domain Name)을 포함할지 여부를 설정합니다. 다음을 선택할 수 있습니다.
  - 디바이스 호스트 이름을 **FQDN**으로 사용
  - 인증서에 **FQDN** 사용 안 함
  - 사용자 정의 **FQDN** - 이 옵션을 선택하고 표시되는 사용자 정의 **FQDN** 필드에서 지정합니다.
- 디바이스의 **IP** 주소 포함 - 인증서 요청에 IP 주소가 포함되는 인터페이스입니다.
- 일반 이름**(CN)** - 인증서에 포함할 X.500 일반 이름입니다.

참고 자체 서명 인증서를 등록할 경우 인증서 파라미터에서 CN(Common Name)을 지정해야 합니다.

- 조직 단위**(OU)** - 인증서에 포함될 조직 단위(부서 등)의 이름입니다.
- 조직**(O)** - 인증서에 포함될 조직 또는 회사 이름입니다.
- 구/군/시**(L)** - 인증서에 포함될 구/군/시입니다.
- 주/도**(ST)** - 인증서에 포함될 주/도입니다.
- 국가 코드**(C)** - 인증서에 포함될 국가입니다. 이 코드는 ISO 3166의 국가 약어를 준수하므로 미국의 경우 "US"로 표시됩니다.
- 이메일**(E)** - 인증서에 포함될 이메일 주소입니다.
- 디바이스의 일련 번호 포함 - 인증서에 디바이스의 인련 번호를 포함할지의 여부입니다. CA는 인증서 인증 또는 추후 특정 디바이스와 인증서를 연결하기 위해 일련 번호를 사용합니다. 확실하지 않은 경우 일련 번호를 포함하면 디버깅 시 유용합니다.

인증서 등록 개체 키 옵션

Secure Firewall Management Center 탐색 경로

개체 > 개체 관리로 이동한 뒤 탐색창에서 **PKI > Cert Enrollment(**인증서 등록**)**를 선택합니다. **Add Cert Enrollment(**인증서 등록 추가**)** 대화 상자를 열고 **(+) Add Cert Enrollment(**인증서 등록 추가**)**를 누른 뒤 **Key(**키**)** 탭을 누릅니다.

필드

- 키 유형—RSA, ECDSA, EdDSA.

참고

- EST 등록 유형의 경우 지원되지 않으므로 EdDSA 키를 선택하지 마십시오.
- EdDSA는 사이트 간 VPN 토폴로지에서만 지원됩니다.
- EdDSA는 원격 액세스 VPN의 ID 인증서로 지원되지 않습니다.

- **Key Name(**키 이름**)** - 인증서와 연결할 키 쌍이 이미 있는 경우, 이 필드는 해당 키 쌍의 이름을 지정합니다. 키 쌍이 존재하지 않는 경우, 이 필드는 등록 중에 생성될 키 쌍에 할당할 이름을 지정합니다. 이름을 지정하지 않으려면 FQDN(Fully Qualified Domain Name) 키 페어를 대신 사용합니다.
- 키 크기 - 키 페어가 존재하지 않는 경우 비트 단위로 원하는 키 크기(모듈러스)를 지정합니다. 권장되는 크기는 2048 비트입니다. 모듈러스 크기가 클수록 키가 안전합니다. 그러나 모듈러스 크기가 큰 키는 생성 및 교환 프로세스에 더 오랜 시간이 걸립니다.(512비트보다 큰 경우 1분 이상)

중요

- management center 및 threat defense 버전 7.0 이상에서는 2048 비트보다 작은 RSA 키 크기의 인증서와 RSA 암호화 알고리즘이있는 SHA-1을 사용하는 키를 등록할 수 없습니다. 그러나 약한 암호로 인증서의 PKI 등록를 사용하여 SHA-1을 RSA 암호화 알고리즘 및 더 작은 키 크기로 사용하는 인증서를 허용할 수 있습니다.
- 약한 암호화 옵션을 활성화하더라도 threat defense 7.0에 대해 2048 비트보다 작은 크기의 RSA 키를 생성할 수 없습니다.

- 고급 설정 - IPsec 리모트 클라이언트 인증서의 키 사용 및 확장 키 사용 확장 값을 검증하지 않는 경우 **Ignore IPsec Key Usage(IPsec** 키 사용 무시**)**를 선택합니다. IPsec 클라이언트 인증서를 확인하는 키 사용을 억제할 수 있습니다. 기본적으로 이 옵션은 활성화되어 있지 않습니다.

참고 사이트 간 VPN 연결의 경우, Windows Certificate Authority(CA)를 사용한다면 기본 애플리케이션 정책 확장은 **IP** 보안 **IKE** 중급입니다. 이 기본 설정을 사용한다면, 선택한 개체에 **Ignore IPsec Key Usage(IPsec** 키 사용량 무시**)** 옵션을 선택해야 합니다. 그렇지 않으면 엔드포인트에서 사이트 간 VPN 연결을 완료할 수 없습니다.

약한 암호로 인증서의 **PKI** 등록

SHA-1 해싱 시그니처 알고리즘 및 인증용 2048 비트보다 작은 RSA 키 크기는 management center 및 threat defense 버전 7.0 이상에서 지원되지 않습니다. 2048 비트보다 작은 RSA 키 크기의 인증서는 등록할 수 없습니다.

7.0보다 낮은 버전을 실행하는 management center 7.0 관리 threat defense에서 이러한 제한을 재정의하려면 threat defense에서 약한 암호화 활성화 옵션을 사용할 수 있습니다. 약한 암호화 키는 키 크기가 큰 키와 같이 안전하지 않으므로 이 키를 허용하지 않는 것이 좋습니다.

참고 Threat Defense 7.0 이상 버전은 약한 암호화를 허용하더라도 2048 비트보다 작은 크기의 RSA 키 생성을 지원하지 않습니다.

디바이스에서 약한 암호화를 활성화하려면 **Devices (**디바이스**)> Certificates (**인증서**)** 페이지로 이동합니다. threat defense 디바이스에 대해 제공된 **Enable Weak-Crypto(**약한 암호화 활성화**)** (🔒) 버튼을 클릭합니다. 약한 암호화 옵션이 활성화되면 버튼이 🔓로 변경됩니다. 기본적으로 약한 암호화 옵션은 사용되지 않습니다.

참고 약한 암호화 사용으로 인해 인증서 등록이 실패하면 management center에 약한 암호화 옵션을 활성화하라는 경고 메시지가 표시됩니다. 마찬가지로, 약한 암호화 활성화 버튼을 켜면 management center가 디바이스에서 약한 암호화 구성을 활성화하기 전에 경고 메시지가 표시됩니다.

이전 버전을 **Threat Defense 7.0**으로 업그레이드

threat defense 7.0으로 업그레이드하는 경우 기존 인증서 구성이 유지됩니다. 그러나 해당 인증서에 2048 비트보다 작은 RSA 키가 있고 SHA-1 암호화 알고리즘을 사용하는 경우에는 VPN 연결을 설정하는 데 사용할 수 없습니다. 2048 비트보다 큰 RSA 키 크기의 인증서를 구매하거나 VPN 연결에 대해 약한 암호화 허용 옵션을 활성화해야 합니다.

인증서 등록 개체 폐기 옵션

방법을 선택 및 구성하여 인증서의 폐기 상태 확인 여부를 지정합니다. 인증서 폐기 확인은 기본적으로 사용하지 않으며 두 방법(CRL 또는 OSCP) 모두 체크 해제되어 있습니다.

Secure Firewall Management Center 탐색 경로

개체 > 개체 관리로 이동한 뒤 탐색창에서 **PKI > PKI** 등록을 선택합니다. **PKI** 등록 추가 대화 상자를 열고 **(+) PKI** 등록 추가를 누른 뒤 폐기 탭을 누릅니다.

필드

- **CRL(Certificate Revocation List)** 활성화 - CRL 확인 활성화 여부를 확인합니다.
  - 인증서에서 **CRL** 배포 지점 사용 - 인증서에서 폐기 목록 배포 URL을 사용하는지 확인합니다.
  - 정적 **URL** 구성 사용 - 폐기 목록에 정적, 사전 정의 배포 URL을 추가하려는 경우 선택합니다. 이어서 URL을 추가합니다.

    CRL 서버 **URL** - CRL을 다운로드할 수 있는 LDAP 서버의 URL입니다.

URL은 **ldap://**, **http://** 또는 **https://**로 시작해야 합니다. URL에 포트 번호를 포함합니다.

- **OCSP(Online Certificate Status Protocol)** 활성화 - OCSP 확인 활성화 여부를 확인합니다.

  OCSP 서버 **URL** - OCSP 확인이 필요한 경우 폐기를 위한 OCSP 서버 확인 URL입니다.

  URL은 **http://** 또는 **https://**로 시작해야 합니다.

- 폐기 정보를 찾을 수 없는 경우 인증서를 유효한 것으로 간주 - 기본적으로 선택되어 있습니다. 이를 허용하지 않으려면 선택을 취소합니다.

참고 **Consider the certificate valid if revocation information cannot be reached(**해지 정보에 연결할 수 없는 경우 인증서를 유효한 것으로 간주**)** 확인란은 버전 6.5 이상을 실행하는 threat defense 디바이스에 영향을 주지 않습니다.

정책 목록

정책 목록 설정 페이지를 사용해 정책 목록 정책 개체를 생성, 복사, 편집할 수 있습니다. 경로 맵을 구성할 때 정책 목록 개체를 생성할 수 있습니다. 경로 맵 내에서 정책 목록이 참조되는 경우 정책 목록의 모든 일치 문장이 평가 및 처리됩니다. 경로 맵 내에 둘 이상의 정책 목록을 구성할 수 있습니다. 정책 목록은 같은 경로 맵 내에 있으나 정책 목록 밖에서 구성된 기존 일치 항목 및 설정 명령문과도 공존할 수 있습니다. 여러 정책 목록이 하나의 경로 맵 항목 내에서 일치를 수행하는 경우 모든 정책 목록은 들어오는 특성에 대해서만 확인됩니다.

이 개체는 threat defense 디바이스와 함께 사용할 수 있습니다.

프로시저

단계 **1** 개체 > 개체 관리를 선택하고 목차에서 정책 목록을 선택합니다.

단계 **2** **Add Policy List(**정책 목록 추가**)**를 클릭합니다.

단계 **3** **Name(**이름**)** 필드에 정책 목록 개체의 이름을 입력합니다. 개체 이름은 대소문자를 구분하지 않습니다.

단계 **4** 작업 드롭다운 목록에서 조건 일치에 대해 액세스를 허용 또는 차단할지 여부를 선택합니다.

단계 **5** 인터페이스 탭을 클릭하여 다음 홉이 지정된 인터페이스 중 하나를 벗어난 경로를 배포합니다.

Zones/Interfaces(영역/인터페이스**)** 목록에서 디바이스가 관리 스테이션과 통신하는 인터페이스가 포함된 영역을 추가합니다. 영역에 없는 인터페이스의 경우 **Selected Zone/Interface(**선택한 영역/ 인터페이스**)** 목록 아래의 필드에 인터페이스 이름을 입력하고 **Add(**추가**)**를 클릭할 수 있습니다. 선택한 인터페이스 또는 영역이 디바이스에 포함되어 있는 경우에만 디바이스에서 호스트가 구성됩니다.

단계 **6** 주소 탭에서 표준 액세스 목록 또는 접두사 목록에서 허용한 대상 주소가 있는 모든 경로를 재배포합니다.

일치시키는 데 사용할 액세스 목록 또는 접두사 목록 중 하나를 선택하고 이때 사용할 표준 액세스 목록 개체 또는 접두사 목록 개체를 입력하거나 선택합니다.

단계 **7** 다음 홉 탭을 클릭하여 지정된 액세스 목록 또는 접두사 목록이 전달한 다음 홉 라우터 주소가 있는 모든 경로를 재배포합니다.

일치시키는 데 사용할 액세스 목록 또는 접두사 목록 중 하나를 선택하고 이때 사용할 표준 액세스 목록 개체 또는 접두사 목록 개체를 입력하거나 선택합니다.

단계 **8** 경로 소스 탭을 클릭하여 액세스 목록 또는 접두사 목록에서 지정된 주소의 라우터 및 액세스 서버가 알려준 경로를 재배포합니다.

일치시키는 데 사용할 액세스 목록 또는 접두사 목록 중 하나를 선택하고 이때 사용할 표준 액세스 목록 개체 또는 접두사 목록 개체를 입력하거나 선택합니다.

단계 **9** BGP 자율 시스템 경로를 일치시키려면 **AS** 경로 탭을 클릭합니다. 하나 이상의 AS 경로를 지정하면 경로는 모든 AS 경로에 대해 일치시킬 수 있습니다.

단계 **10** **Community Rule(**커뮤니티 규칙**)** 탭을 클릭하여 BGP 커뮤니티 또는 확장 커뮤니티를 지정된 커뮤니티 목록 개체 또는 확장 커뮤니티 목록 개체와 각각 일치시킬 수 있습니다. 둘 이상의 규칙을 지정하는 경우 일치하는 허용 또는 거부가 충족될 때까지 규칙에 대해 경로가 확인됩니다.

a) 규칙에 커뮤니티 목록을 지정하려면 **Selected Community List(**선택한 커뮤니티 목록**)** 필드에서 지정된 **Edit(**수정**)** (✎) 항목을 클릭합니다. 커뮤니티 목록이 **Available Community List(**사용 가능한 커뮤니티 목록**)**에 나타납니다. 필요한 목록을 선택하고 **Add(**추가**)**를 클릭한 다음 **OK(**확인**)**를 클릭합니다.

특정 커뮤니티와 BGP 커뮤니티를 정확하게 일치시키려면 **Match the specified community exactly(**지정된 커뮤니티를 정확하게 일치**)** 확인란을 선택합니다.

b) 확장 커뮤니티 목록을 추가하려면 **Selected Extended Community List(**선택한 확장 커뮤니티 목록**)** 필드에서 지정된 **Edit(**수정**)** (✎) 항목을 클릭합니다. 확장 커뮤니티 목록이 **Available Extended Community List(**사용 가능한 확장 커뮤니티 목록**)**에 나타납니다. 필요한 목록을 선택하고 **Add(**추가**)**를 클릭한 다음 **OK(**확인**)**를 클릭합니다.

참고 확장 커뮤니티 목록은 경로 가져오기 또는 내보내기 구성에만 적용됩니다.

단계 **11** 경로의 메트릭 및 보안 그룹 태그와 일치시키려면 메트릭 **&** 태그 탭을 클릭합니다.

a) 메트릭 필드에 일치에 사용할 메트릭 값을 입력합니다. 여러 값을 쉼표로 구분하여 입력할 수 있습니다. 이 설정을 통해 지정된 메트릭이 있는 어떤 값과도 일치시킬 수 있습니다. 메트릭 값의 범위는 0~4294967295입니다.

b) 태그 필드에 일치에 사용할 태그 값을 입력합니다. 여러 값을 쉼표로 구분하여 입력할 수 있습니다. 이 설정을 사용하면 특정 보안 그룹 태그가 있는 모든 경로를 일치시킬 수 있습니다. 태그 값의 범위는 0~4294967295입니다.

단계 **12** 이 개체에 대한 재정의를 허용하려면 **Allow Overrides(**재정의 허용**)** 확인란을 선택합니다. 개체 재정의 허용, 13 페이지의 내용을 참조하십시오.

단계 **13** **Save(**저장**)**를 클릭합니다.

포트

포트 개체는 여러 프로토콜을 조금씩 다른 방법으로 나타냅니다.

TCP 및 UDP

투명 레이어 프로토콜로서 괄호 안에 프로토콜 번호 및 관련 포트 또는 포트 범위가 선택적으로 표시되는 포트 개체입니다. 예: `TCP(6)/22`

ICMP, ICMPv6 (IPv6-ICMP)

인터넷 레이어 프로토콜 및 유형과 코드가 선택적으로 표시되는 포트 개체입니다. 예: `ICMP(1):3:3`

유형이나 가능한 경우 코드로 ICMP 또는 IPV6-ICMP 포트 개체를 제한할 수 있습니다. ICMP 유형 및 코드에 대한 자세한 내용은 다음을 참조하십시오.

- http://www.iana.org/assignments/icmp-parameters/icmp-parameters.xml
- http://www.iana.org/assignments/icmpv6-parameters/icmpv6-parameters.xml

기타

포트를 사용하지 않는 다른 프로토콜을 나타내는 포트 개체입니다.

시스템은 잘 알려진 포트에 기본 포트 개체를 제공합니다. 이런 포트 개체는 수정하거나 삭제할 수 없습니다. 기본 개체에 추가해 사용자 정의 포트 개체를 만들 수 있습니다.

액세스 제어 정책, ID 규칙, 네트워크 검색 규칙, 포트 변수, 이벤트 검색 등 시스템 웹 인터페이스의 다양한 위치에서 포트 개체 및 그룹을 사용할 수 있습니다. 예를 들어, 조직에서 특정 포트 범위를 사용하는 사용자 지정 클라이언트를 사용하며 시스템에서 잘못된 이벤트를 과도하게 생성하는 경우, 이러한 포트의 모니터링을 제외하도록 네트워크 검색 정책을 구성할 수 있습니다.

포트 개체를 사용할 경우 다음 지침을 준수합니다.

- 액세스 제어 규칙에서 소스 포트 조건의 TCP 또는 UDP 이외의 다른 프로토콜을 추가할 수 없습니다. 또한, 규칙에서 소스 및 대상 포트 조건을 모두 설정할 때 전송 프로토콜을 조합할 수 없습니다.
- 소스 포트 조건에서 사용되는 포트 개체 그룹에 지원되지 않는 프로토콜을 추가한 경우 정책 적용 시 사용되는 규칙은 관리되는 디바이스에 반영되지 않습니다.
- 또한, TCP와 UDP 포트를 모두 포함하는 포트 개체를 만들고 이를 규칙의 소스 포트 조건으로 추가하는 경우 대상 포트를 추가할 수 없으며, 그 반대도 마찬가지입니다.

포트 개체 생성

프로시저

단계 **1** **Objects(**개체**)** > **Object Management(**개체 관리**)**을(를) 선택합니다.

단계 **2** 개체 유형 목록에서 **Port(**포트**)**를 선택합니다.

단계 **3** 드롭다운 목록의 **Add Port(**포트 추가**)**에서 **Add Object(**개체 추가**)**를 선택합니다.

단계 **4** **Name(**이름**)**을 입력합니다.

단계 **5** **Protocol(**프로토콜**)**을 선택합니다.

단계 **6** 선택한 프로토콜에 따라 제한할 포트또는 ICMP 유형 및 코드를 선택합니다.

1 에서 **65535**까지의 포트를 입력할 수 있습니다. 포트 범위를 지정하려면 하이픈을 사용합니다. 기타 드롭다운 목록을 사용해 모든 프로토콜에 일치하도록 선택한 경우 포트에 따라 개체를 제한해야 합니다.

단계 **7** 개체에 대한 재정의를 관리합니다.

- 이 개체에 대한 재정의를 허용하려면 **Allow Overrides(**재정의 허용**)** 확인란을 선택합니다. 개체 재정의 허용, 13 페이지의 내용을 참조하십시오.
- 이 개체에 재정의 값을 추가하려면 Override(재정의) 섹션을 펼치고 **Add(**추가**)**를 클릭합니다. 개체 재정의 추가, 14 페이지의 내용을 참조하십시오.

단계 **8** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

- 활성 정책이 개체를 참조하는 경우 구성 변경 사항을 구축합니다. 참조.

포트 개체 가져오기

포트 개체 가져 오기에 대한 자세한 내용은 개체 가져오기, 5 페이지를 참고하십시오.

접두사 목록

경로 맵, 정책 맵, OSPF 필터링 또는 BGP 네이버 필터링을 구성할 때 사용할 IPv4 및 IPv6용 접두어 목록 개체를 만들 수 있습니다.

IPv6 접두사 목록 구성

IPv6 접두사 목록 구성 페이지를 사용하여 접두사 목록 개체를 생성, 복사, 편집합니다. 경로 맵, 정책 맵, OSPF 필터링 또는 BGP 네이버 필터링을 구성할 때 사용할 접두어 목록 개체를 만들 수 있습니다.

이 개체는 threat defense 디바이스와 함께 사용할 수 있습니다.

프로시저

단계 **1** 개체 > 개체 관리를 선택하고 목차에서 접두사 목록 > **IPv6** 접두사 목록을 선택합니다.

단계 2 **Add Prefix List(**접두사 목록 추가**)**를 선택합니다.

단계 3 **New Prefix List Object(**새 접두사 목록 개체**)** 창에서 **Name(**이름**)** 필드에 접두사 목록 개체에 대한 이름을 입력합니다.

단계 4 새 접두사 목록 개체 창에서 **Add(**추가**)**를 클릭합니다.

단계 5 **Action(**작업**)** 드롭다운 목록에서 재배포 액세스를 표시하기 위해 허용 또는 차단 등 적절한 작업을 선택합니다.

단계 6 개체에 이미 구성된 접두사 목록 항목의 목록 내 새 접두사 목록 항목의 위치를 나타내는 고유한 번호를 **Sequence No.(**시퀀스 번호**)** 필드에 입력합니다. 비워 둘 경우 시퀀스 번호는 현재 사용되는 시퀀스 번호보다 5로 기본 설정됩니다.

단계 7 **IP** 주소 필드에 IP 주소/마스크 길이 형식의 IPv6 주소를 지정합니다. 마스크 길이는 1~128 사이의 유효한 값이어야 합니다.

단계 8 **Minimum Prefix Length(**최소 접두사 길이**)** 필드에 최소 접두사 길이를 입력합니다. 이 값은 마스크 길이보다 커야하며 최대 접두사 길이를 지정한 경우 이와 같거나 짧아야 합니다.

단계 9 **Maximum Prefix Length(**최대 접두사 길이**)** 필드에 최대 접두사 길이를 입력합니다. 최소 접두사 길이를 지정한 경우 이 값은 최소 접두사 길이와 같거나 길어야 하며 최소 접두사 길이가 지정되지 않은 경우 마스크 길이보다 길어야 합니다.

단계 10 **Add(**추가**)**를 클릭합니다.

단계 11 이 개체에 대한 재정의를 허용하려면 **Allow Overrides(**재정의 허용**)** 확인란을 선택합니다. 개체 재정의 허용, 13 페이지의 내용을 참조하십시오.

단계 12 **Save(**저장**)**를 클릭합니다.

IPv4 접두사 목록 구성

IPv4 접두사 목록 구성 페이지를 사용하여 접두사 목록 개체를 생성, 복사, 편집합니다. 경로 맵, 정책 맵, OSPF 필터링 또는 BGP 네이버 필터링을 구성할 때 사용할 접두어 목록 개체를 만들 수 있습니다.

이 개체는 threat defense 디바이스와 함께 사용할 수 있습니다.

프로시저

단계 1 **Objects(**개체**)** > **Object Management(**개체 관리**)**를 선택하고 목차에서 **Prefix Lists(**접두사 목록**)** > **IPv4 Prefix List(IPv4** 접두사 목록**)**를 선택합니다.

단계 2 **Add Prefix List(**접두사 목록 추가**)**를 선택합니다.

단계 3 **New Prefix List Object(**새 접두사 목록 개체**)** 창에서 **Name(**이름**)** 필드에 접두사 목록 개체에 대한 이름을 입력합니다.

단계 4 **Add(**추가**)**를 클릭합니다.

단계 5 **Action(**작업**)** 드롭다운 목록에서 재배포 액세스를 표시하기 위해 허용 또는 차단 등 적절한 작업을 선택합니다.

단계 **6** 개체에 이미 구성된 접두사 목록 항목의 목록 내 새 접두사 목록 항목의 위치를 나타내는 고유한 번호를 **Sequence No.(**시퀀스 번호**)** 필드에 입력합니다. 비워 둘 경우 시퀀스 번호는 현재 사용되는 시퀀스 번호보다 5로 기본 설정됩니다.

단계 **7** **IP address(IP** 주소**)** 필드에 IP 주소/마스크 길이 형식의 IPv4 주소를 지정합니다. 마스크 길이 1~32 사이의 유효한 값이어야 합니다.

단계 **8** **Minimum Prefix Length(**최소 접두사 길이**)** 필드에 최소 접두사 길이를 입력합니다. 이 값은 마스크 길이보다 커야하며 최대 접두사 길이를 지정한 경우 이와 같거나 짧아야 합니다.

단계 **9** **Maximum Prefix Length(**최대 접두사 길이**)** 필드에 최대 접두사 길이를 입력합니다. 최소 접두사 길이를 지정한 경우 이 값은 최소 접두사 길이와 같거나 길어야 하며 최소 접두사 길이가 지정되지 않은 경우 마스크 길이보다 길어야 합니다.

단계 **10** **Add(**추가**)**를 클릭합니다.

단계 **11** 이 개체에 대한 재정의를 허용하려면 **Allow Overrides(**재정의 허용**)** 확인란을 선택합니다. 개체 재정의 허용, 13 페이지의 내용을 참조하십시오.

단계 **12** **Save(**저장**)**를 클릭합니다.

경로 맵

경로 맵은 경로를 라우팅 프로세스에 재분배할 때 사용됩니다. 또한 라우팅 프로세스로 기본 경로를 생성할 때도 사용됩니다. 경로 맵은 지정된 라우팅 프로토콜에서 대상 라우팅 프로세스로 재배포를 허용할 경로를 정의합니다. 경로 맵을 구성하여 경로 맵 개체에 대한 새 경로 맵 항목을 생성하거나 기존 경로 맵을 편집합니다.

이 개체는 threat defense 디바이스와 함께 사용할 수 있습니다.

시작하기 전에

A 경로 맵은 이러한 개체를 하나 이상 사용할 수 있습니다. 이런 개체를 모두 추가하는 것은 필수 사항이 아닙니다. 경로 맵을 구성하려면 필요에 따라 이런 개체를 생성하고 사용합니다.

- ACL 추가
- 접두사 목록 추가
- AS 경로 추가
- 커뮤니티 목록 추가
- 확장 커뮤니티 목록을 추가합니다.

참고 확장 커뮤니티 목록은 경로 가져오기 또는 내보내기 구성에만 적용됩니다.

- 정책 목록 추가

프로시저

단계 **1** 개체 > 개체 관리를 선택하고 목차에서 경로 맵을 선택합니다.

단계 **2** **Add Route Map(**경로 맵 추가**)**를 클릭합니다.

단계 **3** **New Route Map Object(**새 경로 맵 개체**)** 창에서 **Add(**추가**)**를 클릭합니다.

단계 **4** **Sequence No.(**시퀀스 번호**)** 필드에 0~65535 사이의 숫자를 입력합니다. 이는 경로 맵 개체에 대해 이미 구성된 경로 맵 항목 목록에 있는 새 경로 맵 항목의 위치를 표시합니다.

참고 나중에 절을 추가해야 할 경우에 대비하여 최소 10개 간격으로 절에 번호를 매기는 것이 좋습니다.

단계 **5** **Redistribution(**재배포**)** 드롭다운 목록에서 재배포 액세스를 표시하기 위해 허용 또는 차단 등 적절한 작업을 선택합니다.

단계 **6** (경로/트래픽을) 일치시키기 위해 목차에서 다음 기준에 따라 **Match Clauses(**절 일치**)** 탭을 클릭합니다.

- **Security Zones(**보안 영역**)** - (인그레스/이그레스) 인터페이스를 기준으로 트래픽에 일치시킵니다. 영역을 선택하여 추가하거나 인터페이스 이름에 입력해 추가합니다.
- **IPv4** - 다음 기준을 기반으로 IPv4(경로/트래픽)을 일치시킵니다. 기준을 정의하려면 탭을 선택합니다.
  1. 경로 주소를 기반으로 경로를 일치시키려면 주소 탭을 클릭합니다. IPv4 주소를 드롭다운 목록에서 일치시키는 데 액세스 목록 또는 접두사 목록을 사용할지 선택하고 이때 사용할 ACL 개체 또는 접두사 목록 개체를 입력하거나 선택합니다.
  2. 경로의 다음 홉 주소를 기반으로 경로를 일치시키려면 다음 홉 탭을 클릭합니다. IPv4 주소를 드롭다운 목록에서 일치시키는 데 액세스 목록 또는 접두사 목록을 사용할지 선택하고 이때 사용할 ACL 개체 또는 접두사 목록 개체를 입력하거나 선택합니다.
  3. 경로의 알림 소스 주소를 기반으로 경로를 일치시키려면 경로 소스 탭을 클릭합니다. IPv4 주소를 드롭다운 목록에서 일치시키는 데 액세스 목록 또는 접두사 목록을 사용할지 선택하고 이때 사용할 ACL 개체 또는 접두사 목록 개체를 입력하거나 선택합니다.
- **IPv6** - 라우팅 주소, 다음 홉 주소, 경로의 알림 소스 주소를 기반으로 IPv6(경로/트래픽)를 일치시킵니다.
- **BGP** - 다음 기준을 기반으로 BGP(경로/트래픽)을 일치시킵니다. 기준을 정의하려면 탭을 선택합니다.
  1. 특정 경로 액세스 목록과 BGP 자율 시스템 경로 액세스 목록 일치를 활성화하려면 **AS** 경로 탭을 클릭합니다. 경로 액세스 목록을 하나 이상 지정하는 경우 경로가 아무 경로 액세스 목록과도 일치할 수 있습니다.
  2. **Community List(**커뮤니티 목록**)** 탭을 클릭하여 BGP 커뮤니티 또는 확장 커뮤니티를 지정된 커뮤니티 목록 개체 또는 확장 커뮤니티 목록 개체와 각각 일치시킬 수 있습니다.
     - 규칙에 커뮤니티 목록을 지정하려면 **Selected Community List(**선택한 커뮤니티 목록**)** 필드에서 지정된 **Edit(**수정**)** (✎) 항목을 클릭합니다. 커뮤니티 목록이 **Available**

Community List(사용 가능한 커뮤니티 목록**)**에 나타납니다. 필요한 목록을 선택하고 **Add(**추가**)**를 클릭한 다음 **OK(**확인**)**를 클릭합니다. 커뮤니티 목록 개체를 생성하는 방법에 대한 자세한 내용은 커뮤니티 목록, 26 페이지 항목을 참조하십시오.

- 확장 커뮤니티 목록을 추가하려면 **Selected Extended Community List(**선택한 확장 커뮤니티 목록**)** 필드에서 지정된 **Edit(**수정**)** (✎) 항목을 클릭합니다. 확장 커뮤니티 목록이 **Available Extended Community List(**사용 가능한 확장 커뮤니티 목록**)**에 나타납니다. 필요한 목록을 선택하고 **Add(**추가**)**를 클릭한 다음 **OK(**확인**)**를 클릭합니다. 확장 커뮤니티 목록 개체를 생성하는 방법에 대한 자세한 내용은 확장 커뮤니티, 27 페이지 항목을 참조하십시오.

지정된 커뮤니티 목록 개체와 BGP 커뮤니티를 정확하게 일치시키려면 **Match the specified community exactly(**지정된 커뮤니티를 정확하게 일치**)** 확인란을 선택합니다. 이 옵션은 확장 커뮤니티 목록에 적용되지 않습니다.

참고 둘 이상의 규칙을 지정하는 경우 일치하는 허용 또는 거부 조건이 충족될 때까지 규칙에 대해 경로가 확인됩니다. 하나 이상의 Match 커뮤니티와 일치하지 않는 경로는 아웃바운드 경로 맵에 대해 알려지지 않습니다.

3. BGP 정책을 평가하고 처리하도록 경로 맵을 구성하려면 정책 목록 탭을 클릭합니다. 여러 정책 목록이 하나의 경로 맵 항목 내에서 일치를 수행하는 경우 모든 정책 목록은 들어오는 특성에 대해서만 확인됩니다.

- **Others(**기타**)** - 다음 기준에 따라 경로 또는 트래픽을 일치시킵니다.

1. 경로 메트릭 일치를 활성화하려면 메트릭 경로 값 필드에 일치에 사용할 메트릭 값을 입력합니다. 여러 값을 쉼표로 구분하여 입력할 수 있습니다. 이 설정을 통해 지정된 메트릭이 있는 어떤 값과도 일치시킬 수 있습니다. 메트릭 값의 범위는 0~4294967295입니다.
2. 태그 값 필드에 일치에 사용할 태그 값을 입력합니다. 여러 값을 쉼표로 구분하여 입력할 수 있습니다. 이 설정을 사용하면 특정 보안 그룹 태그가 있는 모든 경로를 일치시킬 수 있습니다. 태그 값의 범위는 0~4294967295입니다.
3. 경로 유형 일치를 활성화하려면 적절한 경로 유형 옵션을 체크합니다. 유효한 경로 유형은 External1, External2, Internal, Local, NSSA-External1 및 NSSA-External2입니다. 목록에서 하나 이상의 경로 유형을 선택할 수 있습니다.

단계 **7** 목차에서 선택한 다음 조건에 따라 경로/트래픽을 설정하려면 절 설정 탭을 클릭합니다.

- **Metric Values(**메트릭 값**)** - 대역폭을 설정하기 위해 모든 값을 입력하거나 값을 입력하지 않습니다.

1. 대역폭 필드에 초당 Kbits 단위로 메트릭 값 또는 대역폭을 입력합니다. 유효한 값은 0~4294967295 범위의 정수 값입니다.
2. 대상 라우팅 프로토콜에 대한 메트릭 유형을 지정하려면 메트릭 유형 드롭다운 목록에서 선택합니다. 유효한 값은 내부, 유형 1, 유형 2입니다.

- **BGP Clauses(BGP** 절**)** - 다음 조건에 따라 BGP 경로를 설정합니다. 조건을 정의하려면 탭을 선택합니다.

  1. BGP 경로에 대한 자율 시스템 경로를 변경하려면 **AS** 경로 탭을 클릭합니다.

     1. BGP 경로에 임의의 시스템 자율 경로 문자열을 첨부하려면 첨부된 **AS** 경로 필드에 AS 경로 번호를 입력합니다. 일반적으로 로컬 AS 번호가 여러 번 부착되어 자율 시스템 경로 길이가 늘어납니다. AS 경로 번호를 하나 이상 지정하면 경로는 아무 AS 번호나 추가할 수 있습니다.
     2. 최종 AS 번호를 AS 경로에 첨부하려면 최종 **AS**를 **AS** 경로에 첨부 필드에 AS 경로 번호를 입력합니다. AS 번호로 1 ~ 10의 값을 입력하십시오.
     3. **Convert route tag into AS Path(AS** 경로로 경로 태그 변환**)** 확인란을 선택하여 경로의 태그를 자율 시스템 경로로 변환하십시오.

  2. 커뮤니티 속성을 설정하려면 **Community List(**커뮤니티 목록**)** 탭을 클릭합니다.

     Specific Community(특정 커뮤니티**)**에서:

     1. **None(**없음**)**을 클릭하여 경로 맵을 전달하는 접두사에서 커뮤니티 속성을 제거합니다.
     2. **Specify Community(**커뮤니티 설정**)**를 클릭하여 적용 가능한 경우 커뮤니티 번호를 입력합니다. 유효한 값은 1~4294967295입니다.
     3. **Add to the existing communities(**기존 커뮤니티에 추가**)**를 선택하여 커뮤니티를 이미 존재하는 커뮤니티에 추가합니다.
     4. **Internet(**인터넷**)**, **No-advertise(**알림 없음**)** 또는 **No-export(**내보내지 않음**)** 체크 박스를 선택하여 잘 알려진 커뮤니티 중 하나를 사용합니다.

     Specific Extended Community(특정 확장 커뮤니티**)** 아래의 **Route Target(**경로 대상**)** 필드에 경로 대상 번호를 *ASN:nn* 형식으로 입력합니다.

     - 1:1~65534:65535 범위의 값을 입력할 수 있습니다.

       단일 항목에서 단일 경로 대상 또는 쉼표로 구분된 경로 대상 세트를 추가할 수 있습니다. 예: *1:2,1:4,1:6*.

     - 항목에 최대 8개의 경로 대상을 포함할 수 있습니다.
     - 경로 맵에서 중복 경로 대상 항목을 포함할 수 없습니다.

  3. 추가 특성을 설정하려면 기타 탭을 클릭합니다.

     1. 자동으로 태그 값을 계산하려면 자동 태그 설정을 선택합니다.
     2. 로컬 환경설정 설정 필드에 자동 시스템 경로에 대한 환경설정 값을 입력합니다. 0~4294967295 사이의 값을 입력합니다.
     3. 가중치 설정 필드에 라우팅 테이블에 대한 BGP 가중치를 입력합니다. 0에서 65535 사이의 값을 입력합니다.

4. BGP 출처 코드를 지정하려면 선택합니다. 유효한 값은 **Local IGP** Local IGP와 **Incomplete** 입니다.
5. IPv4 설정 섹션에서 패킷이 출력될 다음 홉의 다음 홉 IPv4 주소를 지정합니다. 인접 라우터일 필요는 없습니다. IPv4 주소를 하나 이상 지정하면 패킷이 아무 IP 주소로나 출력될 수 있습니다.

   접두사 목록 드롭다운 목록에서 IPv4 접두사 목록을 지정하려면 이 옵션을 선택합니다.
6. IPv6 설정 섹션에서 하 여 패킷이 출력 되 next hop next hop IPv6 주소를 지정 합니다. 인접 라우터일 필요는 없습니다. IPv6 주소를 둘 이상 지정하면 패킷이 임의 IP 주소로 출력될 수 있습니다.

   접두사 목록 드롭다운 목록에서 IPv6 접두사를 지정하려면 이 옵션을 선택합니다.

단계 **8** **Add(**추가**)**를 클릭합니다.

단계 **9** 이 개체에 대한 재정의를 허용하려면 **Allow Overrides(**재정의 허용**)** 확인란을 선택합니다. 개체 재정의 허용, 13 페이지의 내용을 참조하십시오.

단계 **10** **Save(**저장**)**를 클릭합니다.

보안 인텔리전스

보안 인텔리전스 기능을 사용하려면 위협 라이선스(threat defense 디바이스용) 또는 보호 라이선스(기타 모든 디바이스 유형)가 있어야 합니다.

보안 인텔리전스 목록 및 피드는 목록 또는 피드의 항목과 일치하는 트래픽을 빠르게 필터링하는 데 사용할 수 있는 IP 주소, 도메인 이름 및 URL의 모음입니다.

- 목록은 수동으로 관리하는 정적 컬렉션입니다.
- 피드는 HTTP 또는 HTTPS의 간격에 따라 업데이트되는 동적 컬렉션입니다.

보안 인텔리전스 목록/피드는 다음과 같이 그룹화됩니다.

- DNS(도메인 이름)
- 네트워크(IP 주소)
- URL

시스템에서 제공한 피드

Cisco에서는 다음과 같은 피드를 보안 인텔리전스 개체로 제공합니다.

- 보안 인텔리전스 피드가 Talos에서 최신 위협 인텔리전스로 정기적으로 업데이트됩니다.
  - Cisco-DNS-and-URL-Intelligence-Feed(DNS 목록 및 피드 아래)

- Cisco-Intelligence-Feed(IP 주소의 경우, 네트워크 목록 및 피드 아래)

  시스템에서 제공한 피드는 삭제할 수 없지만 업데이트 빈도는 변경(또는 비활성화)할 수 있습니다.

- Cisco-TID-Feed(네트워크 목록 및 피드 아래)

  이 피드는 액세스 제어 정책의 Security Intelligence(보안 인텔리전스) 탭에서 사용되지 않습니다.

  대신 이 피드를 사용하도록 Secure Firewall 위협 정보 디렉터를 활성화하고 설정해야 합니다. 이 피드는 TID 관찰 가능 데이터의 모음입니다.

  이 개체를 사용하여 이 데이터가 TID 요소에 게시되는 빈도를 설정합니다.

사전 정의된 목록**:** 전역 차단 목록 및 전역 차단 안 함 목록

시스템은 도메인(DNS), IP 주소(네트워크) 및 URL에 대해 사전 정의된 전역 차단 목록 및 차단 안 함 목록과 함께 제공됩니다.

이러한 목록은 사용자가 입력할 때까지 비어 있습니다. 이러한 목록을 작성하려면 글로벌 및 도메인 보안 인텔리전스 목록, 78 페이지의 내용을 참조하십시오.

기본적으로, 액세스 제어 및 DNS 정책은 이러한 목록을 보안 인텔리전스의 일부로 사용합니다.

커스텀 피드

타사 피드를 사용하거나 내부 맞춤형 피드를 통해 여러 Secure Firewall Management Center 어플라이언스를 포함하는 대규모 구축에서 전사적인 차단 목록을 손쉽게 유지 관리할 수 있습니다.

맞춤형 보안 인텔리전스 피드, 84 페이지의 내용을 참조하십시오.

맞춤형 목록

맞춤형 목록은 피드 및 Global(전역) 목록을 보강 및 세부 조정할 수 있습니다.

맞춤형 보안 인텔리전스 목록, 86 페이지의 내용을 참조하십시오.

보안 인텔리전스 목록 및 피드 사용처

- IP 주소 및 주소 블록 — 액세스 제어 정책에서 보안 인텔리전스의 일부로 차단 및 차단 안 함 목록을 사용합니다.
- 도메인 이름 — DNS 정책에서 보안 인텔리전스의 일부로 차단 및 차단 안 함 목록을 사용합니다.
- URL — 액세스 제어 정책에서 보안 인텔리전스의 일부로 차단 및 차단 안 함 목록을 사용합니다. 보안 인텔리전스 이후에 분석 및 트래픽 처리 단계가 발생하는 액세스 제어 및 QoS 규칙에서도 URL 목록을 사용할 수 있습니다.

보안 인텔리전스 개체 수정 방법

차단 목록, 차단 금지 목록, 피드 또는 싱크홀 개체에서 항목을 추가하거나 삭제하려면 다음을 수행합니다.

개체 유형	기능 편집	편집 후 재구축이 필요합니까?
맞춤형 차단 및 차단 금지 목록	개체 관리자를 사용해 새 항목 또는 교체 항목을 업로드합니다.	아니요
기본(단 사용자가 생성한) 차단 및 차단 금지 목록: 전역, 하위, 도메인별	컨텍스트 메뉴를 사용하여 항목을 추가하거나 개체 관리자를 사용하여 항목을 삭제합니다.	아니요
시스템에서 제공한 인텔리전스 피드	개체 관리자를 사용해 빈도 업데이트를 변경 또는 비활성화합니다.	아니요
맞춤 피드	개체 관리자를 사용해 완전히 수정합니다.	아니요
싱크홀	개체 관리자를 사용해 완전히 수정합니다.	예

글로벌 및 도메인 보안 인텔리전스 목록

Firepower Management Center는 네트워크의 이벤트에서 언제든지 URL, 도메인 및 IP 주소를 즉시 추가할 수 있는 빈 전역 차단 및 차단 안 함 목록과 함께 제공됩니다. 이러한 목록을 사용하면 보안 인텔리전스를 통해 특정 연결을 항상 차단하거나 보안 인텔리전스로 인해 특정 연결이 차단되지 않도록 하여 설정한 다른 위협 탐지 프로세스에서 해당 연결을 평가할 수 있습니다.

익스플로잇 시도와 결합된 침입 이벤트에서 라우팅 가능한 IP 주소 집합이 발견되면 해당 IP 주소를 즉시 차단할 수 있습니다. 변경 사항을 전파하기까지 몇 분 정도 걸릴 수 있으나, 재구축하지 않아도 됩니다.

기본적으로, 액세스 제어 및 DNS 정책은 모든 보안 영역에 적용되는 이러한 전역 목록을 사용합니다. 정책별 기준으로 이러한 목록을 사용하지 않도록 선택할 수 있습니다.

참고 이러한 옵션은 보안 인텔리전스에만 적용됩니다. 보안 인텔리전스는 이미 단축 경로가 지정된 트래픽을 차단할 수 없습니다. 마찬가지로, 보안 인텔리전스의 차단 안 함 목록에 항목을 추가해도 일치하는 트래픽을 자동으로 신뢰하거나 단축 경로 지정을 수행하지 않습니다. 자세한 내용은 보안 인텔리전스 정보를 참고하십시오.

다중 도메인 구축의 경우, 도메인 목록은 물론 전역 목록에 항목을 추가하여 차단 또는 보안 인텔리전스 차단에서 제외를 시행하려는 Firepower System 도메인을 선택할 수 있습니다(보안 인텔리전스 목록 및 멀티테넌시, 79 페이지 참조).

보안 인텔리전스 목록 및 멀티테넌시

다중 도메인 구축에서 전역 도메인은 전역 차단 목록 및 차단 안 함 목록을 소유합니다. 전역 관리자만 전역 목록에 항목을 추가하거나 전역 목록에서 항목을 제거할 수 있습니다. 따라서 서브도메인 사용자는 네트워크, 도메인 이름, URL을 차단 및 차단 안 함 목록에 추가할 수 있도록 멀티테넌시는 다음을 추가합니다.

- 도메인 목록 — 특정 서브도메인에만 적용되는 콘텐츠가 있는 차단 또는 차단 안 함 목록입니다. 전역 목록은 전역 도메인에 대한 도메인 목록입니다.
- 하위 도메인 목록 — 현재 도메인이 보유한 하위 항목의 도메인 목록을 집계하는 차단 또는 차단 안 함 목록입니다.

도메인 목록

전역 목록에 액세스할 수 있는 기능(단, 수정 안 됨) 외에도, 각 서브도메인에는 해당 서브도메인에만 적용되는 콘텐츠인 자체 명명된 목록이 있습니다. 예를 들어 Company A로 명명된 서브도메인은 다음을 소유합니다.

- 도메인 차단 목록 - Company A 및 도메인 차단 안 함 목록 - Company A
- DNS에 대한 도메인 차단 목록 - Company A, DNS에 대한 도메인 차단 안 함 목록 - Company A
- URL에 대한 도메인 차단 목록 - Company A, URL에 대한 도메인 차단 안 함 목록 - Company A

현재 도메인 수준 또는 그 이상에 있는 모든 관리자는 이 목록을 입력할 수 있습니다. 콘텍스트 메뉴를 사용하여 현재 및 모든 하위 도메인의 항목을 차단 또는 차단 안 함 목록에 추가할 수 있습니다. 그러나 연결된 도메인의 관리자만 도메인 목록에서 항목을 제거할 수 있습니다.

예를 들어 전역 관리자는 전역 도메인 및 Company A의 도메인에 있는 동일한 IP 주소를 차단 목록에 추가하도록 선택할 수 있으나, Company B의 도메인에 있는 IP 주소는 차단 목록에 추가할 수 없습니다. 이 작업을 수행하면 동일한 IP 주소가 다음 목록에 추가됩니다.

- 전역 차단 목록(전역 관리자만 제거할 수 있는 목록임)
- 도메인 차단 목록 - Company A(Company A 관리자만 제거할 수 있는 목록임)

시스템은 각 리프 도메인에 대해 별도의 네트워크 맵을 작성합니다. 다중 도메인 구축에서 리터럴 IP 주소를 사용하여 이 컨피그레이션을 제한하면 예기치 않은 결과가 발생할 수 있습니다.

하위 도메인 목록

하위 도메인 목록은 현재 도메인이 보유한 하위 항목의 도메인 목록을 집계하는 차단 안 함 또는 차단 목록입니다. 리프 도메인은 하위 도메인 목록을 보유하지 않습니다.

하위 도메인 목록은 더 높은 수준의 도메인 관리자가 일반적인 보안 인텔리전스 설정을 시행할 수 있는 동시에, 서브도메인 사용자가 자체 구축 시 차단 또는 차단 안 함 목록에 항목을 추가할 수 있으므로 유용합니다.

예를 들어 전역 도메인은 다음과 같은 하위 도메인 목록을 보유합니다.

- 하위 차단 목록 - 전역, 하위 차단 안 함 목록 - 전역

- DNS에 대한 하위 차단 목록 - 전역, DNS에 대한 하위 차단 목록 - 전역
- URL에 대한 하위 차단 목록 - 전역, URL에 대한 하위 차단 목록 - 전역

참고 하위 도메인 목록은 수동으로 입력된 목록이 아니라 심볼릭 집계이므로 개체 관리자에 표시되지 않습니다. 하위 도메인 목록은 이를 사용할 수 있는 곳인 액세스 제어 및 DNS 정책에 표시됩니다.

전역 보안 인텔리전스 목록에 항목 추가

이벤트 및 대시 보드를 검토할 때 미리 정의된 차단 목록에 추가하여 해당 이벤트에 나타나는 IP 주소, 도메인 및 URL과 관련된 향후 트래픽을 즉시 차단할 수 있습니다.

마찬가지로 보안 인텔리전스 차단 이후에 위협 탐지 프로세스에서 평가하려는 트래픽을 차단하는 경우 사전 정의된 Do Not Block(차단 금지) 목록에 이벤트의 IP 주소, 도메인 및 URL을 추가할 수 있습니다.

트래픽은 위협 탐지의 보안 인텔리전스 단계에서 이러한 목록의 항목과 비교하여 평가됩니다.

이 목록에 대한 자세한 내용은 글로벌 및 도메인 보안 인텔리전스 목록, 78 페이지의 내용을 참조하십시오.

시작하기 전에

보안 인텔리전스 목록에 항목을 추가하면 액세스 제어에 영향을 미치므로, 다음 사용자 역할 중 한 가지를 보유하고 있어야 합니다.

- 관리자
- 역할의 조합: Network Admin(네트워크 관리자) 또는 Access Admin(액세스 관리자), Security Analyst(보안 분석가) 및 Security Approver(보안 승인자)
- Modify Access Control Policy(액세스 제어 정책 수정) 및 Deploy Configuration to Devices(디바이스에 컨피그레이션 구축) 권한이 모두 있는 맞춤형 역할

해당하는 경우, 이러한 목록이 사용될 것으로 예상되는 정책에 사용되는지 확인합니다.

프로시저

단계 **1** 보안 인텔리전스를 사용하여 항상 차단하거나 보안 인텔리전스 차단에서 제외할 IP 주소, 도메인 또는 URL을 포함하는 이벤트로 이동합니다.

단계 **2** IP 주소, 도메인 또는 URL을 마우스 오른쪽 버튼으로 클릭하고 적절한 옵션을 선택합니다.

항목 유형	상황 메뉴 옵션
IP 주소	차단 목록에 IP 추가 차단 안 함 목록에 IP 추가 이러한 옵션은 IP 주소를 네트워크의 각 목록에 추가합니다.
URL	URL의 전역 차단 목록에 URL 추가 URL의 전역 차단 안 함 목록에 URL 추가
URL 필드에 있는 URL의 도메인	URL의 전역 차단 목록에 도메인 추가 URL의 전역 차단 안 함 목록에 도메인 추가
DNS 쿼리 필드의 도메인	DNS의 전역 차단 목록에 도메인 추가 DNS의 전역 차단 안 함 목록에 도메인 추가

다음에 수행할 작업

이러한 변경 사항을 적용하기 위해 재구축할 필요는 없습니다.

목록에서 항목을 삭제하려면 전역 보안 인텔리전스 목록에서 항목 삭제, 81 페이지의 내용을 참조하십시오.

전역 보안 인텔리전스 목록에서 항목 삭제

참고

- 다중 도메인 구축에서 이러한 목록의 이름은 "Global"이 아닐 수 있습니다. 자세한 내용은 보안 인텔리전스 목록 및 멀티테넌시, 79 페이지를 참고하십시오.
- 이러한 목록에 항목을 추가하려면 전역 보안 인텔리전스 목록에 항목 추가, 80 페이지의 내용을 참조하십시오.

프로시저

단계 **1** **Objects(**개체**)** > **Object Management(**개체 관리**)**를 선택합니다.

단계 **2** **Security Intelligence(**보안 인텔리전스**)**를 클릭합니다.

단계 **3** 적절한 옵션을 클릭합니다.

- **Network Lists and Feeds(**네트워크 목록 및 피드**)**(IP 주소용)
- **DNS** 목록 및 피드(도메인 이름용)
- **URL Lists and Feeds(URL** 목록 및 피드**)**

단계 **4** Global Block(전역 차단) 또는 Global Do-Not-Block(전역 차단 안 함) 목록 옆의 연필을 클릭합니다.

단계 **5** 삭제할 항목 옆의 휴지통 버튼을 클릭합니다.

보안 인텔리전스 목록 및 피드 업데이트

목록 및 피드 업데이트는 기존 목록을 대체하거나 파일에 새 파일의 내용을 피드합니다. 기존 및 새로운 파일의 내용은 병합되지 않습니다.

시스템이 손상된 피드 또는 인식할 수 있는 항목이 없는 피드를 다운로드하는 경우, (처음 다운로드가 아니라면) 시스템은 오래된 피드 데이터를 사용하여 계속 진행합니다. 그러나 시스템이 피드에서 항목을 하나라도 인식할 수 있는 경우, 인식할 수 있는 항목을 사용합니다.

기본적으로 피드는 매 2시간마다 Management Center를 업데이트합니다. 빈도는 수정할 수 있습니다. Management Center가 수신하는 모든 업데이트는 즉시 매니지드 디바이스로 전달됩니다. 또한 매니지드 디바이스는 30분마다 FMC를 폴링하여 변경 사항을 확인합니다. 이 빈도는 수정할 수 없습니다.

다중 도메인 구축에서 시스템이 제공한 피드 전역 도메인에 속하고 해당 도메인의 관리자만 수정할 수 있습니다. 사용자의 도메인에 속한 사용자 정의 피드의 업데이트 빈도는 수정할 수 있습니다.

피드 업데이트 간격을 수정하려면 보안 인텔리전스 피드에 대한 업데이트 빈도 변경, 82 페이지의 내용을 참조하십시오.

보안 인텔리전스 피드에 대한 업데이트 빈도 변경

Firepower Management Center가 보안 인텔리전스 피드를 업데이트하는 간격을 지정할 수 있습니다.

피드 업데이트에 대한 자세한 내용은 보안 인텔리전스 목록 및 피드 업데이트, 82 페이지의 내용을 참조하십시오.

프로시저

단계 **1** **Objects(**개체**)** > **Object Management(**개체 관리**)**을(를) 선택합니다.

단계 **2** 보안 인텔리전스 노드를 확장하고 빈도를 변경하고 싶은 피드 유형을 선택합니다.

시스템에서 제공하는 URL 피드는 **DNS Lists and Feeds(DNS** 목록 및 피드**)** 아래의 도메인 피드와 결합됩니다.

단계 **3** 업데이트하고자 하는 피드 옆에 있는 **Edit(**수정**)** ( )을 클릭합니다.

View(보기**)** ( )가 대신 표시되는 경우에는 개체가 상위 도메인에 속하거나 개체를 수정할 권한이 없는 것입니다.

단계 **4** **Update Frequency(**업데이트 빈도**)**를 수정합니다.

단계 **5** **Save(**저장**)**를 클릭합니다.

사용자 지정 보안 인텔리전스 목록 및 피드

사용자 지정 목록 및 피드: 요구 사항

목록 및 피드 포맷

각 목록 또는 피드는 500MB 이하의 간단한 텍스트 파일이어야 합니다. 목록 파일은 .txt 확장자를 사용해야 합니다. 한 줄당 하나의 항목 또는 코멘트를 포함합니다(IP 주소 1개, URL 1개, 도메인 이름 1개).

팁 포함할 수 있는 항목 수는 파일의 최대 크기에 따라 제한됩니다. 예를 들어 코멘트가 없고 평균 URL 길이가 100자(Punycode 또는 퍼센트 Unicode 표시 및 줄바꿈 포함)인 URL 목록에는 524만 개 이상의 항목을 포함할 수 있습니다.

DNS 목록 항목에서 도메인 라벨에 별표(*) 와일드카드 문자를 지정할 수 있습니다. 모든 라벨이 와일드카드와 일치됩니다. 예를 들어 `www.example.*` 항목은 `www.example.com` 및 `www.example.co`와 모두 일치됩니다.

소스 파일 내에 코멘트 행을 추가할 경우, 해당 행은 파운드(#) 문자로 시작해야 합니다. 코멘트가 있는 소스 파일을 업로드할 경우, 업로드 과정에서 코멘트가 제거됩니다. 다운로드하는 소스 파일에는 코멘트 없이 모든 항목이 포함됩니다.

피드 요건

피드를 구성할 때 URL을 사용하여 해당 위치를 지정합니다. URL은 Punycode로 인코딩된 것이 아니어야 합니다.

피드 업데이트 간격이 30분 이하인 경우 MD5 URL을 지정해야 합니다. 이렇게 하면 변경되지 않은 피드를 자주 다운로드할 수 없습니다. 피드 서버에서 MD5 URL을 제공하지 않는 경우 30분 이상의 다운로드 간격을 사용해야 합니다.

MD5 체크섬을 사용하는 경우 오직 체크섬으로만 간편한 텍스트 파일로 저장해야 합니다. 코멘트가 지원되지 않습니다.

URL 목록 및 피드: URL 구문 및 일치 기준

보안 인텔리전스 URL 목록 및 피드(맞춤형 목록, 피드 및 전역 차단 목록 및 차단 금지 목록의 항목 포함)에는 다음과 같은 내용이 포함될 수 있으며 설명된 바와 같이 일치 동작이 있습니다.

- 호스트 이름

  예를 들어, **www.example.com**이 있습니다.

- URL

  example.com은 **example.com**과 그의 모든 하위 도메인과(**www.example.com**, **eu.example.com**, **example.com/abc** 그리고 **www.example.com/def**을 포함) 일치하지만

example.co.uk, **examplexyz.com**, **example.com.malicious-site.com**과는 일치하지 않습니다.

전체 URL 경로를 포함할 수도 있습니다. 예를 들면 **https://www.cisco.com/c/en/us/products/security/firewalls/index.html**.

- 정확한 일치를 나타내는 URL 끝에 있는 슬래시

  example.com/는 **example.com**과만 일치합니다. **www.example.com** 또는 다른 URL과는 일치하지 않습니다.

- URL의 도메인을 나타내는 와일드 카드(*)

  별표는 점으로 구분된 전체 도메인 문자열을 나타낼 수 있지만 부분 도메인 문자열은 사용할 수 없으며 첫 번째 슬래시 다음에 오는 URL의 어떤 부분도 될 수 없습니다.

  유효한 예:

  - ***.example.com**
  - **www.*.com**
  - 예. *****

    (이는 **example.com** 및 **example.org** 및 **example.de**와 일치하지만 **example.co.uk**와는 일치하지 않습니다.)

  - ***.example.***
  - 예. ***/**

  잘못된 예:

  - **example*.com**
  - **example.com/***

- IP 주소(IPv4)

  IPv6 주소의 경우 또는 범위 또는 CIDR 표기법을 사용하려면 보안 인텔리전스 네트워크 개체를 사용합니다.

  옥텟을 나타내는 하나 이상의 와일드 카드를 포함할 수 있습니다(예: 10.10.10. * 또는 10.10. *. *).

맞춤형 보안 인텔리전스 목록, 86 페이지도 참조하십시오.

맞춤형 보안 인텔리전스 피드

사용자 지정 또는 서드파티 보안 인텔리전스 피드를 사용하면 정기적으로 업데이트되며 평판이 좋은 인터넷의 다른 차단 안 함 목록 및 차단 목록으로 시스템이 제공한 인텔리전스 피드를 보강할 수 있습니다. 하나의 소스 목록을 사용하여 구축 시 여러 Secure Firewall Management Center 어플라이언스를 업데이트할 때 유용한 내부 피드를 설정할 수도 있습니다.

참고 보안 인텔리전스 피드의 /0 넷마스크를 사용하여 주소 블록에 차단 또는 차단 안 함 목록을 추가할 수 없습니다. 정책이 대상으로 하는 모든 트래픽을 모니터링하거나 차단하려는 경우 **Monitor(**모니터링**)** 또는 **Block(**차단**)**인 액세스 제어 규칙을 사용하고 **Source Networks(**소스 네트워크**)** 및 **Destination Networks(**대상 네트워크**)**에는 기본값은 any(모든)을 사용합니다.

시스템이 MD5 체크섬을 사용하도록 구성하여 업데이트된 피드를 다운로드할지 결정할 수도 있습니다. 시스템이 피드를 마지막으로 다운로드한 이후로 체크섬이 변경되지 않는 경우 시스템이 이를 다시 다운로드할 필요는 없습니다. 특히 내부 피드가 클 경우 MD5 체크섬을 사용할 수 있습니다.

참고 시스템은 사용자 지정 피드를 다운로드할 때 피어 SSL 인증서 확인을 수행하지 않습니다. 또한 시스템은 원격 피어를 확인하는 인증서 번들 또는 자체 서명된 인증서를 사용하도록 지원하지 않습니다.

시스템이 인터넷에서 피드를 업데이트할 때 엄격한 제어를 원할 경우, 해당 피드에 대한 자동 업데이트를 비활성화할 수 있습니다. 그러나 자동 업데이트는 가장 연관성 있는 최신 데이터를 지원합니다.

수동으로 보안 인텔리전스 피드를 업데이트하면 인텔리전스 피드를 비롯한 모든 피드가 업데이트됩니다.

사용자 지정 목록 및 피드: 요구 사항, 83 페이지에서 전체 요구 사항을 참조하십시오.

보안 인텔리전스 피드 생성

위협 라이선스(threat defense 디바이스용) 또는 보호 라이선스(기타 모든 디바이스 유형)가 있어야 합니다.

프로시저

단계 **1** **Objects(**개체**)** > **Object Management(**개체 관리**)**을(를) 선택합니다.

단계 **2** 보안 인텔리전스 노드를 확장하고 추가하려는 피드 유형을 선택합니다.

단계 **3** 위에서 선택한 피드 유형에 적절한 옵션을 클릭합니다.

- **Add Network Lists and Feeds(**네트워크 목록 및 피드 추가**)**(IP 주소)
- **ADD DNS Lists and Feeds(DNS** 목록 및 피드 추가**)**
- **URL Lists and Feeds(URL** 목록 및 피드 추가**)**

단계 **4** 피드의 **Name(**이름**)**을 입력합니다.

다중 도메인 구축에서 개체 이름은 도메인 계층 내에서 고유해야 합니다. 시스템은 현재 도메인에서 확인할 수 없는 개체 이름과의 충돌을 식별할 수 있습니다.

단계 **5** **Type(**유형**)** 드롭다운 목록에서 **Feed(**피드**)**를 선택합니다.

단계 **6** 피드 **URL**을 입력합니다.

단계 **7** **MD5 URL**을 입력합니다.

이는 피드 콘텐츠가 마지막 업데이트 이후에 변경되었는지를 확인하는 데 사용되므로 시스템은 변경되지 않은 피드를 다운로드하지 않습니다.

30분 미만의 업데이트 간격에는 MD5 URL이 필요합니다.

피드 서버에서 MD5 URL을 제공하지 않는 경우 30분 이상의 간격을 선택해야 합니다.

단계 **8** **Update Frequency(**업데이트 빈도**)**를 선택합니다.

단계 **9** **Save(**저장**)**를 클릭합니다.
피드 업데이트를 비활성화하지 않는 한, 시스템은 피드를 다운로드하고 확인하려고 시도합니다.

보안 인텔리전스 피드 수동 업데이트

위협 라이선스(threat defense 디바이스용) 또는 보호 라이선스(기타 모든 디바이스 유형)가 있어야 합니다.

시작하기 전에

하나 이상의 디바이스가 관리 센터에 추가되어 있어야 합니다.

프로시저

단계 **1** **Objects(**개체**)** > **Object Management(**개체 관리**)**을(를) 선택합니다.

단계 **2** 보안 인텔리전스 노드를 확장하고 피드 유형을 선택합니다.

단계 **3** 업데이트 피드를 클릭하고 확인합니다.

단계 **4** **OK(**확인**)**를 클릭합니다.

Secure Firewall Management Center는 피드 업데이트를 다운로드 및 확인한 후 변경 사항을 관리되는 디바이스로 전달합니다. 업데이트된 피드를 사용하여 트래픽 필터링이 시작됩니다.

맞춤형 보안 인텔리전스 목록

보안 인텔리전스 목록은 사용자가 시스템에 수동으로 업로드하는 IP 주소와 주소 블록, URL, 도메인 이름에 대한 간단한 정적 목록입니다. Secure Firewall Management Center의 단일 관리되는 디바이스에 대해 전역 목록 중 하나 또는 피드를 보강하고 세부적으로 조정하려는 경우에는 사용자 지정 목록이 유용합니다.

예를 들어, 평판이 좋은 피드가 중요한 리소스에 액세스하는 것을 잘못 차단하고 있지만 사용자 조직에 전반적으로 유용한 경우, IP 주소 피드 개체를 액세스 제어 정책의 차단 목록에서 제거하는 대신 잘못 분류된 IP 주소만 포함하는 사용자 지정 차단 안 함 목록을 생성할 수 있습니다.

참고 보안 인텔리전스 목록의 `/0` 넷마스크를 사용하여 주소 블록에 차단 또는 차단 안 함 목록을 추가할 수 없습니다. 정책이 대상으로 하는 모든 트래픽을 모니터링하거나 차단하려는 경우 **Monitor(**모니터링**)** 또는 **Block(**차단**)**인 액세스 제어 규칙을 사용하고 **Source Networks(**소스 네트워크**)** 및 **Destination Networks(**대상 네트워크**)**에는 기본값은 `any(모든)`을 사용합니다.

목록 항목 서식에 대해서는 다음을 참조하십시오.

- 주소 블록에 대한 넷마스크는 IPv4 및 IPv6의 경우 각각 `0~32` 또는 `0~128`의 정수일 수 있습니다.
- 도메인 이름의 유니코드는 Punycode 형식으로 인코딩되어야 하고 대소문자를 구분하지 않습니다.
- 도메인 이름은 대소문자를 구분하지 않습니다.
- URL의 유니코드는 % 인코딩 형식으로 인코딩되어야 합니다.
- URL의 하위 디렉터리는 대소문자를 구분하지 않습니다.
- 파운드 기호(#)로 시작하는 목록 항목은 설명으로 처리됩니다.
- 사용자 지정 목록 및 피드: 요구 사항, 83 페이지에서 추가 형식 요구 사항을 참조하십시오.

일치 목록 항목은 다음을 참조하십시오.

- 시스템은 URL 또는 DNS 목록에 더 높은 수준의 도메인이 존재하는 경우 하위 도메인을 일치시킵니다. 예를 들어 `example.com`을 DNS 목록에 추가하는 경우 시스템은 `www.example.com` 및 `test.example.com`을 일치시킵니다.
- 시스템은 DNS 또는 URL 목록 항목의 DNS 조회(전달 또는 역방향)은 수행하지 않습니다. 예를 들어 `http://192.168.0.2`를 URL 목록에 추가하고 `http://www.example.com`에서 해제하는 경우 시스템은 `http://192.168.0.2`만 일치시키고 `http://www.example.com`은 일치시키지 않습니다.

새 보안 인텔리전스 목록을 다음에 업로드 **Secure Firewall Management Center**

보안 인텔리전스 목록을 수정하려면 소스 파일을 변경하고 새 복사본을 업로드해야 합니다. 웹 인터페이스를 사용해 파일 내용을 수정할 수 없습니다. 소스 파일에 액세스할 수 없는 경우 시스템에서 복사본을 다운로드할 수 있습니다.

프로시저

단계 **1** **Objects(**개체**)** > **Object Management(**개체 관리**)**을(를) 선택합니다.

단계 **2** 보안 인텔리전스 노드를 확장하고 목록 유형을 선택합니다.

단계 **3** 위에서 선택한 목록에 적절한 옵션을 클릭합니다.

- **Add Network Lists and Feeds(**네트워크 목록 및 피드 추가**)**(IP 주소)
- **ADD DNS Lists and Feeds(DNS** 목록 및 피드 추가**)**
- **URL Lists and Feeds(URL** 목록 및 피드 추가**)**

단계 **4** **Name(**이름**)**을 입력합니다.

다중 도메인 구축에서 개체 이름은 도메인 계층 내에서 고유해야 합니다. 시스템은 현재 도메인에서 확인할 수 없는 개체 이름과의 충돌을 식별할 수 있습니다.

단계 **5** **Type(**유형**)** 드롭다운 목록에서 **List(**목록**)**를 선택합니다.

단계 **6** **Browse(**찾아보기**)**를 클릭하여 목록에서 `.txt` 파일을 탐색한 후 **Upload(**업로드**)**를 클릭합니다.

단계 **7** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

이러한 변경 사항을 적용하기 위해 재구축할 필요는 없습니다. 목록에서 항목을 삭제하려면 전역 보안 인텔리전스 목록에서 항목 삭제, 81 페이지의 내용을 참조하십시오.

보안 인텔리전스 목록 업데이트

다중 도메인 구축에서 시스템은 현재 도메인에서 생성된 개체를 표시하며 이러한 개체는 수정할 수 있습니다. 상위 도메인에서 생성된 개체도 표시되지만, 이러한 개체는 수정할 수 없습니다. 하위 도메인에서 생성된 개체를 보고 수정하려면 해당 도메인으로 전환하십시오.

프로시저

단계 **1** **Objects(**개체**)** > **Object Management(**개체 관리**)**을(를) 선택합니다.

단계 **2** 보안 인텔리전스 노드를 확장하고 목록 유형을 선택합니다.

단계 **3** 업데이트하려는 목록 옆의 **Edit(**수정**)** ( )을 클릭합니다.

View(보기**)** ( )이 대신 표시되는 경우에는 설정이 상위 도메인에 속하거나 설정을 수정할 권한이 없는 것입니다.

단계 **4** 목록 복사본을 편집해야 하는 경우 **Download(**다운로드**)**를 클릭하고 항목을 텍스트 파일로 저장하려면 브라우저 프롬프트를 따릅니다.

단계 **5** 필요에 따라 목록을 변경합니다.

단계 **6** 보안 인텔리전스 팝업 창에서 수정된 목록을 검색하려면 **Browse(**찾아보기**)**를 클릭하고 **Upload(**업로드**)**를 클릭합니다.

단계 **7** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

이러한 변경 사항을 적용하기 위해 재구축할 필요는 없습니다. 목록에서 항목을 삭제하려면 전역 보안 인텔리전스 목록에서 항목 삭제, 81 페이지의 내용을 참조하십시오.

싱크홀

싱크홀 개체는 싱크홀 내의 모든 도메인 이름용으로 라우팅할 수 없는 주소를 제공하는 DNS 서버나 서버로 확인되지 않는 IP 주소를 나타냅니다. DNS 정책 규칙 내의 싱크홀 개체를 참조하여 일치하는 트래픽을 싱크홀로 리디렉션할 수 있습니다. 개체에는 IPv4 주소와 IPv6 주소를 모두 할당해야 합니다.

싱크홀 개체 생성

위협 라이선스(threat defense 디바이스용) 또는 보호 라이선스(기타 모든 디바이스 유형)가 있어야 합니다.

프로시저

단계 **1** **Objects(**개체**)** > **Object Management(**개체 관리**)**을(를) 선택합니다.

단계 **2** 개체 유형 목록에서 **Sinkhole(**싱크홀**)**을 선택합니다.

단계 **3** **Add Sinkhole(**싱크홀 추가**)**을 클릭합니다.

단계 **4** **Name(**이름**)**을 입력합니다.

다중 도메인 구축에서 개체 이름은 도메인 계층 내에서 고유해야 합니다. 시스템은 현재 도메인에서 확인할 수 없는 개체 이름과의 충돌을 식별할 수 있습니다.

단계 **5** 싱크홀의 **IPv4** 주소 및 **IPv6** 주소를 입력합니다.

단계 **6** 다음 옵션을 이용할 수 있습니다.

- 싱크홀 서버로 트래픽을 리디렉션하려면 **Log Connections to Sinkhole(**싱크홀에 대한 연결 로깅**)**을 선택합니다.
- 확인되지 않은 IP 주소로 트래픽을 리디렉션하려면 **Block and Log Connections to Sinkhole(**싱크홀에 대한 연결 차단 및 로깅**)**을 선택합니다.

단계 **7** 싱크홀에 IoC(보안 침해 지표) 유형을 할당하려면 **Type(**유형**)** 드롭다운에서 유형 하나를 선택합니다.

단계 **8** **Save(**저장**)**를 클릭합니다.

SLA 모니터링

각 인터넷 프로토콜 SLA(Service Level Agreement)는 모니터링되는 주소에 대한 연결 정책을 정의하며 주소에 대한 경로의 가용성을 추적합니다. 경로는 ICMP 에코 요청을 전송하고 응답을 기다리며 주기적으로 가용성을 확인합니다. 요청이 시간 초과되면 경로는 라우팅 테이블에서 제거되고 백업 경로로 교체됩니다. SLA 모니터링 작업은 구축 후 즉시 시작되고 SLA 모니터를 디바이스 설정에서 제거하지 않는 이상 계속 실행됩니다. (즉 노후화가 되지 않습니다.) 인터넷 프로토콜 SLA(Service

Level Agreement) 모니터링 개체는 IPv4 정적 경로 정책의 경로 추적 필드에 사용됩니다. IPv6 경로에는 경로 추적을 통해 SLA 모니터를 사용하기 위한 옵션이 없습니다.

이러한 개체는 threat defense 디바이스와 함께 사용할 수 있습니다.

프로시저

단계 **1** 개체 > 개체 관리를 선택하고 목차에서 **SLA** 모니터링을 선택합니다.

단계 **2** **ADD SLA Monitor(SLA** 모니터링 추가**)**를 클릭합니다.

단계 **3** **Name(**이름**)** 필드에 개체의 이름을 입력합니다.

단계 **4** (선택 사항) **Description(**설명**)** 필드에 개체의 설명을 입력합니다.

단계 **5** **Frequency(**빈도**)** 필드에 초 단위로 ICMP 에코 요청 전송의 간격을 입력합니다. 유효한 값은 1~604800초(7일)입니다. 기본값은 60초입니다.

참고 빈도는 시간 초과 값보다 작을 수 없습니다. 값을 비교하려면 빈도를 밀리초 단위로 변경해야 합니다.

단계 **6** **SLA** 모니터 **ID** 필드에 SLA 작업의 ID 번호를 입력합니다. 유효한 값은 1~2147483647입니다. 최대 2000개의 SLA 작업을 생성할 수 있습니다. 각 ID 번호는 정책 및 디바이스 설정에 대해 고유해야 합니다.

단계 **7** 임계값 필드에서 ICMP 에코 요청 후 임계값 증가 선언 전 통과해야 하는 시간을 입력합니다. 유효한 값은 0~2147483647밀리초입니다. 기본값은 5000밀리초입니다. 임계값은 정의된 값을 초과하는 이벤트를 표시할 때만 사용됩니다. 적절한 시간 초과 값을 평가하기 위해 이러한 이벤트를 사용할 수 있습니다. 모니터링되는 주소의 연결성을 직접 표시하지 않습니다.

참고 임계값은 시간 초과 값을 넘지 않아야 합니다.

단계 **8** 시간 초과 필드에 SLA 작업이 ICMP 에코 요청 응답을 대기하는 시간을 밀리초 단위로 입력합니다. 유효한 값은 0~604800000밀리초(7일)입니다. 기본값은 5000밀리초입니다. 이 필드에 정의된 시간 안에 모니터링되는 주소에서 응답이 수신되지 않으면 고정 경로는 라우팅 테이블에서 제거되고 백업 경로로 교체됩니다.

참고 시간 초과 값은 빈도 값을 초과할 수 없습니다. (수치를 비교하기 위해 빈도 값을 밀리초 단위로 조정합니다.)

단계 **9** 데이터 크기 필드에 ICMP 요청 패킷 페이로드의 크기를 바이트 단위로 입력합니다. 유효한 값의 범위는 0~16384바이트입니다. 기본값은 28바이트이며 총 64바이트의 ICMP 패킷을 생성합니다. 프로토콜 또는 경로 최대 전송 단위(PMTU)에 의해 허용되는 최대값보다 큰 값을 설정하지 마십시오. 소스와 대상의 PMTU 변경을 탐지하려면 연결성을 위해 기본 데이터 크기를 늘려야 할 수 있습니다. 낮은 PMTU는 세션 성능에 영향을 미칠 수 있으며 탐지되는 경우 보조 경로를 사용해야 함을 나타냅니다.

단계 **10** **ToS** 필드에 ICMP 요청 패킷의 IP 헤더에서 정의된 서비스 유형(ToS) 값을 입력합니다. 유효한 값의 범위는 0~255입니다. 기본값은 0입니다. 이 필드에는 지연, 우선 순위, 신뢰성 등의 정보가 포함됩니다. 네트워크의 다른 디바이스가 커밋된 액세스 속도 등 정책 라우팅 및 기능에 이를 사용할 수 있습니다.

단계 **11** 패킷 수 필드에 전송되는 패킷 수를 입력합니다. 유효한 값의 범위는 1~100입니다. 기본값은 1패킷입니다.

참고 패킷 손실로 인해 Secure Firewall Threat Defense 디바이스가 모니터링되는 주소에 연결할 수 없다고 잘못 인식하는 것이 우려되는 경우 기본 패킷 수를 늘립니다.

단계 **12** 모니터링 되는 주소 필드에는 SLA 작업을 통해 가용성이 모니터링되는 IP 주소를 입력합니다.

단계 **13** 가용 영역 목록은 영역 및 인터페이스 그룹을 표시합니다. 영역/인터페이스 목록에는 디바이스가 관리 스테이션과 통신하는 인터페이스가 포함된 영역 및 인터페이스 그룹을 추가합니다. 단일 인터페이스를 지정하려면 인터페이스에 영역 또는 인터페이스 그룹을 생성해야 합니다. 보안 영역 및 인터페이스 그룹 개체 생성을 참조하십시오. 디바이스에 선택된 인터페이스 또는 영역이 포함되는 경우에만 디바이스에서 호스트가 구성됩니다.

단계 **14** **Save(**저장**)**를 클릭합니다.

시간 범위

규칙을 적용할 시기를 결정하는 데 사용할 기간을 정의하려면 시간 범위 개체를 사용합니다.

참고 시간 기반 ACL은 management center 7.0부터 Snort 3에서도 지원됩니다.

시간 범위 개체 생성

특정 시간 범위에만 적용되는 정책을 원하는 경우 시간 범위 개체를 생성하고 정책에서 해당 개체를 지정합니다. 이 개체는 threat defense 디바이스에서만 작동합니다.

이 항목의 하단에 나열된 정책 유형에서만 시간 범위 개체를 지정할 수 있습니다.

참고 표준 시간대는 디바이스의 현지 시간을 나타내며, 시간 범위를 지원하는 정책의 규칙에서 시간 범위를 적용하는 데만 사용됩니다. 표준 시간대는 디바이스의 구성된 시간을 변경하지 않습니다. 구성을 확인하려면 threat defense CLI에서 **show time-range timezone** 및 **show time** 명령을 사용합니다(Cisco Secure Firewall Threat Defense 명령 참조 가이드 참조). 또한 섀시의 표준 시간대가 관리 센터의 표준 시간대를 재정의합니다.

시작하기 전에

시간 범위는 트래픽을 처리하는 디바이스와 연결된 표준 시간대를 기준으로 적용됩니다. 기본적으로 UTC입니다. 디바이스와 연결된 표준 시간대를 변경하려면 **Device(**디바이스**) > Platform Settings(**플랫폼 설정**)**로 이동합니다.

프로시저

단계 **1** 개체 > 개체 관리를 선택합니다.

단계 **2** 개체 유형 목록에서 **Time Range(**시간 범위**)**를 선택합니다.

단계 **3** **Add Time Range(**시간 범위 추가**)**를 클릭합니다.

단계 **4** 값을 입력합니다.

다음 지침을 참조하십시오.

- 입력한 개체 이름 주변에 붉은색 오류 상자가 등장하는 경우 이름 필드 위로 마우스를 이동하여 이름 지정 제한 사항을 확인하십시오.
- **Device(**디바이스**) > Platform Settings(**플랫폼 설정**)**에서 디바이스의 표준 시간대를 지정하지 않는 한 모든 시간은 UTC로 표시됩니다.
- 24시간을 사용하여 시간을 입력합니다. 예를 들어 오후 1시 30분은 13시30분으로 입력합니다.
- 일반적인 주말 시간(저녁과 밤을 포함해 금요일 오후 5시부터 월요일 오전 8시까지)같은 단일 연속 범위를 지정하려면 범위 유형에서 **Range(**범위**)**를 선택합니다.
- 월요일부터 금요일까지 오전 8시부터 오후 5시까지(매일 저녁, 밤, 이른 아침 포함)와 같은 여러 날짜의 일부분만 지정하려면 범위 유형에서 **Daily Interval(**매일 간격**)**을 선택합니다.
- 단일 개체에서 최대 28개의 기간을 지정할 수 있습니다.
- 하루 중 연속되지 않는 시간 또는 며칠 동안 다른 시간대를 지정하려면 복수의 반복 간격을 생성합니다. 예를 들어 표준 근무 시간 외 항상 정책을 적용하려면 다음과 같은 두 가지 반복 간격을 포함하는 단일 시간 범위 개체를 생성합니다.
  - 월요일부터 금요일 오전 9시부터 오후 5시까지 매일 간격
  - 금요일 오후 5시부터 월요일 오전 8시까지 범위 반복 간격

단계 **5** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

다음 중 하나에서 시간 범위를 설정합니다.

- 액세스 제어 규칙
- 사전 필터 규칙
- 터널 규칙
- VPN 그룹 정책

VPN 그룹 정책 개체에서 **Access Hours(**액세스 시간**)** 필드를 사용하여 시간 범위 개체를 지정합니다. 자세한 내용은 그룹 정책 개체 설정, 118 페이지 및 그룹 정책 고급 옵션, 125 페이지 섹션을 참조해 주십시오.

시간대

매니지드 디바이스의 로컬 표준 시간대를 지정하려면 표준 시간대 개체를 생성하고 디바이스에 할당된 디바이스 플랫폼 설정 정책에 해당 개체를 지정합니다.

이 디바이스 로컬 시간은 액세스 제어, 사전 필터 및 VPN 그룹 정책과 같이 시간 범위를 지원하는 정책의 규칙에 시간 범위를 적용하는 데만 사용됩니다. 디바이스에 표준 시간대를 할당하지 않으면 이러한 정책에서 시간 범위를 적용할 때 UTC가 기본적으로 사용됩니다. 시스템의 다른 기능은 표준 시간대 개체에 지정된 표준 시간대를 사용하지 않습니다.

표준 시간대 개체는 threat defense 디바이스에서만 지원됩니다.

참고 시간 기반 ACL은 management center 7.0부터 Snort 3에서도 지원됩니다.

터널 영역

터널 영역은 특별한 분석을 위해 명시적으로 태그를 지정하는 특정 유형의 일반 텍스트, 패스쓰루 터널을 나타냅니다. 터널 영역은 일부 컨피그레이션에서 인터페이스 제약 조건으로 사용할 수 있지만 인터페이스 개체는 아닙니다.

자세한 내용은 터널 영역 및 사전 필터링를 참조하십시오.

URL

중요 보안 인텔리전스 설정에서 이 옵션 및 이와 유사한 옵션을 사용하는 방법 및 액세스 제어 및 QoS 정책의 URL 규칙에 대한 모범 사례는 수동 URL 필터링 옵션의 내용을 참조하십시오.

URL 개체는 단일 URL 또는 IP 주소를 정의하는 반면 URL 그룹 개체는 여러 URL 또는 주소를 정의할 수 있습니다. 액세스 제어 정책 및 이벤트 검색을 포함해 시스템 웹 인터페이스의 여러 위치에서 URL 개체 및 그룹을 사용할 수 있습니다.

URL 개체를 생성할 때는 다음 사항에 유의하십시오.

- 경로를 포함하지 않는 경우(즉, URL에 / 문자가 없음), 이 일치는 서버의 호스트 이름만을 기준으로 합니다. 호스트 이름은 :// 구분자 뒷부분 또는 호스트 이름의 의 뒷부분이 같아야 일치하는 것으로 간주됩니다. 예를 들어 ign.com은 ign.com 및 www.ign.com과 일치하지만 verisign.com과는 일치하지 않습니다.

- 하나 이상의 / 문자를 포함하는 경우, 전체 URL 문자열이 서버 이름, 경로 및 쿼리 파라미터를 비롯한 부분 문자열 일치에 사용됩니다. 그러나 서버가 재구성되고 페이지가 새 경로로 이동될 수 있으므로 개별 웹 페이지 또는 사이트 일부를 차단하거나 허용하기 위해 수동 URL 필터링은 사용하지 않는 것이 좋습니다. 부분 문자열 일치는 예기치 않은 일치로 이어질 수도 있으며, 이 경우에는 URL 개체에 포함하는 문자열도 쿼리 파라미터 내부에 있는 의도하지 않은 서버 또는 문자열의 경로와 일치됩니다.
- 시스템에서는 암호화 프로토콜(HTTP 대 HTTPS)을 무시합니다. 다시 말해, 특정 웹 사이트를 차단하는 경우 애플리케이션 조건을 사용하여 특정 프로토콜을 대상으로 하지 않는 한 해당 웹 사이트에 대한 HTTP 및 HTTPS 트래픽이 모두 차단됩니다. URL 개체를 생성할 때에는 개체 생성 시 프로토콜을 지정할 필요가 없습니다. 이를테면 http://example.com 대신 example.com을 사용하십시오.
- URL 개체를 사용하여 액세스 제어 규칙에서 HTTPS 트래픽을 매칭하려는 경우, 트래픽 암호화에 사용되는 공개 키 인증서에서 주체 CN을 사용하여 개체를 생성합니다. 또한 주체 CN에 포함된 하위 도메인은 무시되므로 하위 도메인 정보를 포함하지 마십시오. 이를테면 www.example.com 대신 example.com을 사용하십시오.

  그러나 인증서의 주체 일반 이름은 웹 사이트의 도메인 이름과 아무런 관련도 없을 수 있습니다. 예를 들어, youtube.com 인증서의 주체 일반 이름은 *.google.com입니다(언제든 변경 가능). URL 필터링 규칙이 암호 해독된 트래픽에서 작동하도록 SSL 암호 해독 정책을 사용하여 HTTPS 트래픽을 암호 해독하면 더 일관성 있는 결과를 얻게 됩니다.

참고 인증서 정보를 더 이상 사용할 수 없어 브라우저에서 TLS 세션을 다시 시작하는 경우에는 URL 개체가 HTTPS 트래픽과 일치되지 않습니다. 따라서 URL 개체를 주의하여 구성하더라도 HTTPS 연결에 대해 일관성 없는 결과를 얻을 수 있습니다.

URL 개체 생성

프로시저

단계 **1** **Objects(**개체**)** > **Object Management(**개체 관리**)**을(를) 선택합니다.

단계 **2** 개체 유형 목록에서 **URL**을 선택합니다.

단계 **3** 드롭다운 목록의 **Add URL(URL** 추가**)**에서 **Add Object(**개체 추가**)**를 선택합니다.

단계 **4** **Name(**이름**)**을 입력합니다.

다중 도메인 구축에서 개체 이름은 도메인 계층 내에서 고유해야 합니다. 시스템은 현재 도메인에서 확인할 수 없는 개체 이름과의 충돌을 식별할 수 있습니다.

단계 **5** 필요한 경우 **Description(**설명**)**을 입력합니다.

단계 **6** **URL** 또는 IP 주소를 입력합니다.

단계 **7** 개체에 대한 재정의를 관리합니다.

- 이 개체에 대한 재정의를 허용하려면 **Allow Overrides(**재정의 허용**)** 확인란을 선택합니다. 개체 재정의 허용, 13 페이지의 내용을 참조하십시오.
- 이 개체에 재정의 값을 추가하려면 Override(재정의) 섹션을 펼치고 **Add(**추가**)**를 클릭합니다. 개체 재정의 추가, 14 페이지의 내용을 참조하십시오.

단계 **8** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

- 활성 정책이 개체를 참조하는 경우 구성 변경 사항을 구축합니다. 참조.

변수 세트

변수는 소스 및 대상 IP 주소와 포트 확인을 위해 침입 규칙에서 일반적으로 사용되는 값을 나타냅니다. 규칙 삭제, 적응형 프로파일 업데이트, 동적 규칙 상태의 IP 주소를 나타내려면 침입 정책 내 변수를 사용할 수도 있습니다.

팁 전처리기 규칙은 침입 규칙에서 사용되는 네트워크 변수에 의해 정의된 호스트에 관계없이 이벤트를 트리거할 수 있습니다.

변수 집합을 사용하여 변수를 관리하고, 사용자 정의하며, 정렬합니다. 시스템이 제공하는 기본 변수 집합을 사용하거나 사용자 정의 집합을 생성할 수 있습니다. 모든 집합에서 사전 정의된 기본 변수를 수정하고 사용자가 정의한 변수를 추가하거나 수정할 수 있습니다.

시스템이 제공하는 대부분의 공유 개체 규칙 및 표준 텍스트 규칙은 사전 정의된 기본 변수를 사용하여 네트워크 및 포트 번호를 정의합니다. 예를 들어, 대부분의 규칙은 `$HOME_NET` 변수를 사용하여 보호된 네트워크를 지정하고 `$EXTERNAL_NET` 변수를 사용하여 보호되지 않은(또는 외부) 네트워크를 지정합니다. 또한, 전문 규칙은 종종 미리 정의된 다른 변수를 사용합니다. 예를 들어, 웹 서버에 대한 익스플로잇을 탐지하는 규칙은 `$HTTP_SERVERS` 및 `$HTTP_PORTS` 변수를 사용합니다.

규칙은 변수가 더 정확하게 네트워크 환경을 반영할 때 더욱 효과적입니다. 적어도 기본 집합의 기본 변수를 수정해야 합니다. `$HOME_NET`과 같은 변수가 올바르게 네트워크를 정의하고 `$HTTP_SERVERS`가 네트워크에서 모든 웹 서버를 포함한다는 것을 확인함으로써 프로세스가 최적화되고 모든 관련 시스템에서 의심스러운 활동이 감시됩니다.

변수를 사용하려면, 액세스 제어 규칙 또는 액세스 제어 정책의 기본 작업과 관련된 침입 정책에 변수 집합을 연결합니다. 기본적으로, 기본 변수 집합은 액세스 제어 정책에 의해 사용된 모든 침입 정책에 연결됩니다.

어느 집합이든 변수를 추가하면 모든 집합에 변수가 추가됩니다. 즉 각 변수 집합은 시스템에서 현재 구성된 모든 변수의 집합입니다. 모든 변수 집합에서 사용자 정의 변수를 추가하거나 모든 변수의 값을 사용자 정의할 수 있습니다.

먼저, 시스템은 단일 기본 변수 집합을 제공하는데, 이는 미리 정의된 기본값으로 구성되어 있습니다. 기본 집합의 각 변수는 초기 기본값으로 설정되는데, 이때 사전 정의된 변수의 경우 Talos 인텔리전스 그룹이 설정하고 규칙 업데이트에서 제공되는 값입니다.

미리 정의된 기본 변수가 해당 기본값으로 구성된 상태로 둘 수도 있지만, Cisco는 사용자가 미리 정의된 변수의 하위 집합을 변경할 것을 권장합니다.

기본 집합에서만 변수를 사용할 수 있지만 대부분의 경우 하나 이상의 사용자 지정 집합을 추가하고, 다양한 집합에서 여러 변수 값을 구성하며, 새로운 변수를 추가하는 것이 유용할 수 있습니다.

여러 집합을 사용할 때, 기본 집합 내 모든 변수의 현재 값이 다른 모든 집합 내 변수의 기본값을 결정한다는 점을 기억하는 것이 중요합니다.

개체 관리자 페이지에서 **Variable Sets(**변수 집합**)**을 선택할 때 개체 관리자는 기본 변수 집합 및 사용자가 생성한 모든 사용자 정의 집합을 나열합니다.

새롭게 설치된 시스템에서 기본 변수 집합은 Cisco가 사전에 정의한 기본 변수만으로 구성됩니다.

각 변수 집합은 시스템이 제공하는 기본 변수와 사용자가 모든 변수 집합에서 추가한 모든 사용자 변수를 포함합니다. 기본 집합을 수정할 수 있지만, 기본 집합을 변경하거나 삭제할 수 없다는 점을 참고하십시오.

다중 도메인 구축의 경우 시스템은 각 하위 도메인에 기본 변수 집합을 생성합니다.

⚠

주의 액세스 제어 정책 또는 침입 정책을 가져오는 경우, 기본 변수 집합의 기존 기본 변수를 가져온 기본 변수로 덮어씁니다. 기존 기본 변수 값 집합이 가져온 기본 변수 값 집합에 없는 사용자 지정 변수를 포함하는 경우, 고유 변수는 유지됩니다.

관련 항목

변수 관리, 108 페이지
변수 집합 관리, 107 페이지

침입 정책 내 변수 집합

기본적으로 Firepower System은 액세스 제어 정책에서 사용되는 모든 침입 정책에 기본 변수 집합을 연결합니다. 침입 정책을 사용하는 액세스 제어 정책을 구축하면 침입 정책에서 활성화한 침입 규칙이 연결된 변수 집합의 변수 값을 사용합니다.

액세스 제어 정책의 침입 정책에서 사용하는 사용자 정의 변수 집합을 수정하면 시스템은 액세스 제어 정책 페이지에서 해당 정책의 상태를 오래된 것으로 표시합니다. 사용자 변수 집합의 변경 내용을 반영하려면 액세스 제어 정책을 재구축해야 합니다. 기본 집합을 변경하면 시스템은 침입 정책을 사용한 모든 액세스 제어 정책의 상태를 오래된 것으로 표시하며 변경 사항을 반영하려면 사용자는 모든 액세스 제어 정책을 재구축해야 합니다.

변수

변수는 다음 범주 중 하나에 속합니다.

기본 변수

Firepower System에서 제공한 변수 기본 변수의 이름을 변경하거나 삭제할 수 없으며, 해당 기본 값을 변경할 수 없습니다. 그러나 기본 변수의 사용자 정의 버전을 만들 수 있습니다.

사용자 정의 변수

사용자가 생성한 변수 다음과 같은 변수를 포함합니다.

- 사용자 지정 기본 변수

  기본 변수 값을 수정할 때, 시스템은 변수를 Default Variables(기본 변수) 영역에서 Customized Variables(사용자 지정 변수) 영역으로 옮깁니다. 기본 집합의 변수 값이 사용자 지정 집합 내 변수의 기본값을 결정하기 때문에, 기본 집합의 기본 변수를 사용자 지정하면 다른 모든 집합 내 변수의 기본값을 수정합니다.

- 사용자 정의 변수

  사용자 고유의 변수를 추가 및 삭제할 수 있으며, 그 값을 다른 변수 집합 내에서 사용자 정의하고, 기본값에 사용자 지정 변수를 재설정할 수 있습니다. 사용자 정의된 변수를 재설정해도 사용자 정의된 변수 영역에 남아 있습니다.

  사용자 정의 변수의 유형은 다음과 같습니다.

  - *network* 변수는 네트워크 트래픽에서 호스트 IP 주소를 지정합니다.
  - *port* 변수는 각 유형에 대한 `any` 값을 포함하여 네트워크 트래픽에서 TCP 또는 UDP 포트를 지정합니다.

예를 들어 사용자 정의 표준 텍스트 규칙을 생성한 경우 트래픽을 정확하게 반영하기 위해 사용자 정의된 변수 또는 규칙 생성 프로세스를 간소화하는 바로가기를 추가하려고 할 수 있습니다. 또는 "비무장 지대"(또는 DMZ)의 트래픽만 검사하는 규칙을 생성하는 경우 해당 값이 노출된 서버 IP 주소를 나열하는 `$DMZ`라는 이름의 변수를 생성할 수 있습니다. 그러면 이 영역에 작성된 모든 규칙에서 `$DMZ` 변수를 사용할 수 있습니다.

고급 변수

Firepower System이 특정 조건에서 제공하는 변수 이러한 변수는 매우 제한적으로 구축됩니다.

사전 정의된 기본 변수

기본적으로 Firepower System은 사전 정의된 기본 값으로 구성된 단일 기본 변수 집합을 제공합니다. Talos 인텔리전스 그룹은 기본 변수를 포함해 신규 및 업데이트된 침입 규칙과 다른 침입 규칙 요소를 제공하기 위해 규칙 업데이트를 사용합니다.

그러나 시스템이 제공하는 대부분의 침입 규칙은 사전 정의된 기본 변수를 사용하므로 이러한 변수에 대해 적절한 값을 설정해야 합니다. 네트워크의 트래픽을 확인하기 위해 변수 집합을 사용하는 방법에 따라 일부 또는 전체 변수 집합에서 이 기본 변수의 값을 수정할 수 있습니다.

주의 액세스 제어 정책 또는 침입 정책을 가져오는 경우, 기본 변수 집합의 기존 기본 변수를 가져온 기본 변수로 덮어씁니다. 기존 기본 변수 값 집합이 가져온 기본 변수 값 집합에 없는 사용자 지정 변수를 포함하는 경우, 고유 변수는 유지됩니다.

다음 표는 시스템이 제공하는 변수 및 일반적으로 수정하는 변수를 나타냅니다. 네트워크에 맞게 변수를 조정하는 방법을 확인하는 데 대한 지원을 받으려면 Professional Services(전문 서비스) 또는 Support(지원부)에 문의하십시오.

표 ***3:*** 시스템 제공 변수

변수 이름	설명	수정 여부
`$AIM_SERVERS`	알려진 AIM(AOL Instant Messenger) 서버에 대해 정의하며 채팅 기반 규칙 및 AIM 익스플로잇을 검색하는 규칙에서 사용됩니다.	필요하지 않음
`$DNS_SERVERS`	DNS(Domain Name Service) 서버에 대해 정의합니다. 특히 DNS 서버에 영향을 미치는 규칙을 작성하는 경우, `$DNS_SERVERS` 변수를 대상 또는 소스 IP 주소로 사용할 수 있습니다.	현재 규칙 집합에서 필요하지 않습니다.
`$EXTERNAL_NET`	Firepower System이 보호되지 않는 네트워크로 간주하는 네트워크에 대해 정의하며 외부 네트워크에 대한 많은 규칙에서 사용됩니다.	예, `$HOME_NET`을 적절하게 정의한 후 `$EXTERNAL_NET`에 대한 값에서 `$HOME_NET`을 제외해야 합니다.
`$FILE_DATA_PORTS`	암호화되지 않은 포트에 대해 정의하며 네트워크 스트림에서 파일을 탐지하는 침입 규칙에서 사용됩니다.	필요하지 않음
`$FTP_PORTS`	네트워크에서 FTP 서버의 포트에 대해 정의하고, FTP 서버 익스플로잇 규칙에 사용됩니다.	FTP 서버가 기본 포트 이외의 포트를 사용할 경우, 예(웹 인터페이스에서 기본 포트를 볼 수 있음).
`$GTP_PORTS`	패킷 디코더가 GTP(GPRS[General Radio Packet Service] 터널링 프로토콜) PDU 내의 페이로드를 추출하는 데이터 채널 포트에 대해 정의합니다.	필요하지 않음
`$HOME_NET`	관련된 침입 정책이 모니터링하는 네트워크에 대해 정의하며, 내부 네트워크를 정의하는 많은 규칙에서 사용됩니다.	예(내부 네트워크에 대한 IP 주소를 포함할 경우)
`$HTTP_PORTS`	네트워크에서 웹 서버의 포트에 대해 정의하고, 웹 서버 익스플로잇 규칙에 사용됩니다.	웹 서버가 기본 포트 이외의 포트를 사용하는 경우, 예(웹 인터페이스에서 기본 포트를 볼 수 있음).
`$HTTP_SERVERS`	네트워크에서 웹 서버에 대해 정의합니다. 웹 서버 익스플로잇 규칙에 사용합니다.	예(HTTP 서버를 실행하는 경우)

변수 이름	설명	수정 여부
$ORACLE_PORTS	네트워크에서 Oracle(오라클) 데이터베이스 서버 포트에 대해 정의하고, Oracle(오라클) 데이터베이스 공격을 검색하는 규칙에서 사용됩니다.	예(Oracle(오라클) 서버를 실행하는 경우)
$SHELLCODE_PORTS	시스템이 셸 코드 코드 익스플로잇을 검색하기를 원하는 포트에 대해 정의하고, 셸 코드를 사용하는 익스플로잇을 탐지하는 규칙에서 사용됩니다.	필요하지 않음
$SIP_PORTS	네트워크에서 SIP 서버 포트에 대해 정의하고, SIP 익스플로잇 규칙에 사용됩니다.	필요하지 않음
$SIP_SERVERS	네트워크에서 SIP 서버에 대해 정의하고, SIP 대상 익스플로잇을 처리하는 규칙에서 사용됩니다.	예(SIP 서버를 실행하는 경우), $HOME_NET을 적절하게 정의한 후 $HOME_NET을 $SIP_SERVERS에 대한 값으로 포함해야 합니다.
$SMTP_SERVERS	네트워크에서 SMTP 서버에 대해 정의하고, 메일 서버를 대상으로 하는 익스플로잇을 해결하는 규칙에서 사용됩니다.	예(SMTP 서버를 실행하는 경우)
$SNMP_SERVERS	네트워크에서 SNMP 서버에 대해 정의하고, SNMP 서버에서 공격을 검색하는 규칙에 사용됩니다.	예(SNMP 서버를 실행하는 경우)
$SNORT_BPF	이후에 5.3.0 이상으로 업그레이드한 Firepower System 소프트웨어 릴리스 5.3.0 이하 시스템에 레거시 고급 변수가 등장하는 경우를 식별합니다.	아니요, 이 변수를 보거나 삭제하는 것만 가능합니다. 삭제한 다음 수정하거나 복원할 수 없습니다.
$SQL_SERVERS	네트워크의 데이터베이스 서버에 대해 정의하고 데이터베이스 대상 익스플로잇을 처리하는 규칙에서 사용됩니다.	예(SQL Server를 실행하는 경우)
$SSH_PORTS	네트워크에서 SSH 서버의 포트에 대해 정의하고, SSH 서버 익스플로잇 규칙에 사용됩니다.	SSH 서버가 기본 포트 이외의 포트를 사용하는 경우, 예(웹 인터페이스에서 기본 포트를 볼 수 있음)
$SSH_SERVERS	네트워크의 SSH 서버에 대해 정의하고 SSH를 대상으로 한 익스플로잇을 해결하는 규칙에서 사용됩니다.	예(SSH 서버를 실행하는 경우), $HOME_NET을 적절하게 정의한 후 $HOME_NET을 $SSH_SERVERS에 대한 값으로 포함해야 합니다.
$TELNET_SERVERS	네트워크에서 알려진 텔넷 서버에 대해 정의하고 텔넷 서버를 대상으로 한 익스플로잇을 해결하는 규칙에 사용됩니다.	예(텔넷 서버를 실행하는 경우)
$USER_CONF	웹 인터페이스를 통해 사용이 불가능한 하나 이상의 기능을 구성하는 일반 도구를 제공합니다. 충돌 또는 중복 $USER_CONF 구성은 시스템을 중단시킵니다.	아니요(기능 설명의 지침에 따른 경우 또는 Support(지원부)의 안내에 따른 경우에만 해당)

네트워크 변수

네트워크 변수는 침입 정책 및 침입 정책 규칙 억제, 다이내믹 규칙 상태 및 적응형 프로파일 업데이트에서 활성화할 수 있는 침입 규칙에서 사용할 수 있는 IP 주소를 나타냅니다. 네트워크 개체 및 네트워크 개체 그룹과 다른 네트워크 변수는 침입 정책 및 침입 규칙에 특정되며 사용자는 네트워크 개체 및 그룹을 사용하여 액세스 제어 정책, 네트워크 변서, 침입 규칙, 네트워크 검색 규칙, 이벤트 검색, 보고서 등 시스템 웹 인터페이스 내 여러 위치의 IP 주소를 대표합니다.

다음 구성의 네트워크 변수를 사용하여 네트워크에 호스트의 IP 주소를 지정할 수 있습니다.

- 침입 규칙 - 침입 규칙 **Source IPs(**소스 **IP)** 및 **Destination IPs(**대상 **IP)** 헤더 필드는 특정 IP 주소에서 시작되었거나 특정 IP 주소로 향하는 패킷 검사를 제한할 수 있습니다.
- 억제 - 소스 또는 대상 침입 규칙 억제의 **Network(**네트워크**)** 필드는 특정 IP 주소 또는 IP 주소 범위가 침입 규칙 또는 프리프로세서를 트리거할 때 침입 이벤트 알림을 억제하도록 할 수 있습니다.
- 다이내믹 규칙 상태 - 소스 또는 대상 다이내믹 규칙 상태의 **Network(**네트워크**)** 필드는 지정된 기간 동안 하나의 침입 규칙 또는 프리프로세서 규칙에 대한 일치가 과도하게 발생하는 경우를 탐지합니다.
- 적응형 프로파일 업데이트 - 적응형 프로파일 업데이트를 활성화하면, 적응형 프로파일 네트워크 필드는 패킷 프래그먼트 및 TCP 스트림의 리어셈블리를 개선하는 호스트를 식별합니다.

이 섹션에서 식별된 필드에 변수를 사용할 때, 사용자가 침입 정책에 연결하는 변수 집합은 침입 정책을 사용하는 액세스 제어 정책에 의해 처리된 네트워크 트래픽에서 변수 값을 결정합니다.

변수에 다음 네트워크 구성의 모든 조합을 추가할 수 있습니다:

- 네트워크 변수, 네트워크 개체 및 사용 가능한 네트워크 목록에서 선택하는 네트워크 개체 그룹의 조합
- New Variable(새 변수) 페이지 또는 Edit Variable(변수 수정) 페이지에서 추가한 후 사용자 변수 및 기타 기존 및 이후 변수에 추가할 수 있는 개별 네트워크 개체
- 리터럴, 단일 IP 주소 또는 주소 블록

  여러 리터럴 IP 주소 및 주소 블록 각각을 개별적으로 추가하여 나열할 수 있습니다. IPv4 및 IPv6 주소와 주소 블록을 단독으로 또는 조합하여 나열할 수 있습니다. IPv6 주소를 지정할 때, RFC 4291에 정의된 주소 지정 규칙을 사용할 수 있습니다.

추가한 모든 변수의 네트워크에 포함된 기본값은 `any`이며, 이는 모든 IPv4 또는 IPv6 주소를 나타냅니다. 제외된 네트워크 기본값은 없으며 이는 네트워크 없음을 나타냅니다. 또한 포함된 네트워크 목록에서 모든 IPv6 주소를 나타내는 리터럴 값으로, 또는 제외 목록에서 IPv6 주소 없음으로 주소 `::`를 지정할 수 있습니다.

제외한 목록에 네트워크를 추가하면 지정된 주소 및 주소 블록을 무효화합니다. 즉 제외된 IP 주소 또는 주소 블록을 제외한 모든 IP 주소와 일치시킬 수 있습니다.

예를 들어, 리터럴 주소 `192.168.1.1`을 제외하면 192.168.1.1을 제외한 모든 IP 주소가 지정되며, `2001:db8:ca2e::fa4c`를 제외하면 2001:db8:ca2e::fa4c를 제외한 모든 IP 주소가 지정됩니다.

리터럴 또는 가용 네트워크를 사용하여 모든 네트워크의 조합을 제외할 수 있습니다. 리터럴 값 `192.168.1.1`과 `192.168.1.5`를 제외하면 192.168.1.1 또는 192.168.1.5 이외의 IP 주소를 포함합니다. 즉 시스템은 이를 "192.168.1.1이 아니고 192.168.1.5도 아닌 것"으로 해석하며, 이는 괄호 사이에 나열된 IP 주소를 제외한 모든 IP 주소에 일치하는 것입니다.

네트워크 변수를 추가하거나 수정할 때는 다음 사항에 유의하십시오.

- 논리적으로 `any` 값을 제외할 수 없습니다. 제외할 경우, 이는 어떤 주소도 나타내지 않습니다. 예를 들면 제외된 네트워크의 목록에 값 `any`의 변수를 추가할 수 없습니다.
- 네트워크 변수는 지정된 침입 규칙 및 침입 정책 기능의 트래픽을 식별합니다. 전처리기 규칙은 침입 규칙에서 사용되는 네트워크 변수에 의해 정의된 호스트에 관계없이 이벤트를 트리거할 수 있습니다.
- 제외된 값은 포함된 값의 하위 집합을 확인해야 합니다. 예를 들어, 192.168.5.0/24 주소 블록을 포함하거나 192.168.6.0/24를 제외할 수 없습니다.

포트 변수

포트 변수는 사용자가 침입 정책에서 활성화한 침입 규칙 내 **Source Port(**소스 포트**)** 및 **Destination Port(**대상 포트**)** 헤더 필드에서 사용할 수 있는 TCP 및 UDP 포트를 나타냅니다. 포트 변수는 포트 개체 및 포트 개체 그룹과 달리 침입 규칙에 특정적입니다. TCP 및 UDP에 대한 포트 개체를 생성할 수 있고 포트 변수, 액세스 제어 정책, 네트워크 검색 규칙, 이벤트 검색 등 시스템 웹 인터페이스의 여러 위치에서 포트 개체를 사용할 수 있다.

특정 TCP 또는 UDP 포트에서 오거나 그 포트로 이동하는 패킷으로 패킷 검사를 제한하려면 **Source Port** 및 **Destination Port** 헤더 필드의 침입 규칙에서 포트 변수를 사용할 수 있습니다.

이 필드에 변수를 사용할 때, 액세스 제어 규칙 또는 정책과 관련된 침입 정책에 연결한 변수 집합은 액세스 제어 정책을 적용하는 네트워크 트래픽에서 해당 변수의 값을 결정합니다.

변수에 다음 포트 구성의 모든 조합을 추가할 수 있습니다

- 사용 가능한 포트 목록에서 선택하는 포트 변수 및 포트 개체의 모든 조합

  사용 가능한 포트 목록이 포트 개체 그룹을 표시하지 않는다는 점과 변수에 이를 추가할 수 없다는 점에 주의하십시오.

- New Variable(새 변수) 페이지 또는 Edit Variable(변수 수정) 페이지에서 추가한 후 사용자 변수 및 기타 기존 및 이후 변수에 추가할 수 있는 개별 포트 개체

  각 유형의 `any` 값을 포함하여 TCP 및 UDP 포트만이 유효한 변수 값입니다. 유효한 변수 값이 아닌 유효한 포트 개체를 추가하기 위해 새 변수 페이지 또는 변수 수정 페이지를 사용할 경우, 개체는 시스템에 추가되지만 가용 개체 목록에 표시되지 않습니다. 개체 관리자를 사용하여 변수에 사용되는 포트 개체를 수정할 때, 유효한 변수 값에 대해 값을 변경하기만 할 수 있습니다.

- 단일, 리터럴 포트 값 및 포트 범위

  대시(-)로 포트 범위를 구분해야 합니다. 콜론(:)으로 표시된 포트 범위는 이전 버전 호환성을 위해 지원되지만 사용자가 생성하는 포트 변수에 콜론을 사용할 수 없습니다.

  여러 리터럴 포트 값 및 범위를 어떤 조합에서나 각각 개별적으로 추가하여 나열할 수 있습니다.

포트 변수를 추가하거나 수정할 때는 다음 사항에 유의하십시오.

- 추가한 모든 변수의 포트에 포함된 기본값은 `any`이며, 이는 모든 포트 또는 포트 범위를 나타냅니다. 제외한 포트에 대한 기본값은 `none`이며, 이는 아무 포트도 없음을 나타냅니다.

팁 값 `any`의 변수를 생성하려면 특정 값을 추가하지 않은 채 변수의 이름을 지정하고 저장하십시오.

- 논리적으로 `any` 값을 제외할 수 없습니다. 제외할 경우, 이는 어떤 포트도 나타내지 않습니다. 예를 들어 제외된 포트의 목록에 값 `any`의 변수를 추가하면 변수 집합을 저장할 수 없습니다.
- 제외한 목록에 포트를 추가하면 지정된 포트 및 포트 범위가 무효화됩니다. 즉 제외된 포트 또는 포트 범위를 제외한 모든 포트와 일치시킬 수 있습니다.
- 제외된 값은 포함된 값의 하위 집합을 확인해야 합니다. 예를 들어, 포트 범위 10-50을 포함하거나 포트 60을 제외할 수 없습니다.

고급 변수

고급 변수는 웹 인터페이스를 통해 구성해야 하는 기능을 구성할 수 있습니다. Firepower System은 현재 하나의 고급 변수인 USER_CONF 변수만 제공합니다.

USER_CONF

USER_CONF는 웹 인터페이스를 통해 구성해야 하는 하나 이상의 기능을 구성하는 일반 도구를 제공합니다.

주의 기능 설명에서 또는 Support(지원부)를 통해 침입 정책 기능을 구성하라는 안내를 받지 않은 한 침입 정책 기능을 구성하기 위해 USER_CONF 고급 변수를 사용하지 마십시오. 충돌이나 이중 설정은 시스템을 중단시킵니다.

USER_CONF를 수정할 때, 단일 회선에 총 최대 4096개의 문자를 입력할 수 있습니다. 회선은 자동으로 래핑됩니다. 디스크 공간과 같은 변수 또는 물리적 제한을 위한 8192개의 최대 문자 길이에 도달할 때까지 유효한 지침 또는 회선을 원하는 만큼 포함할 수 있습니다. 명령 지시어의 모든 전체 인수 뒤에 백슬래시(\) 줄 연속 문자를 사용합니다.

USER_CONF를 재설정하면 빈 상태로 남게 됩니다.

변수 재설정

새 변수 페이지 또는 변수 수정 페이지에서 변수 집합의 기본값에 변수를 재설정할 수 있습니다. 다음 표는 변수 재설정의 기본 원칙에 대해 요약합니다.

표 *4:* 변수 재설정 값

재설정할 변수 유형	집합 유형	재설정
기본	기본값	규칙 업데이트 값
사용자 정의	기본값	any
기본 또는 사용자 정의	사용자 지정	현재 기본 설정값(변경되거나 변경되지 않은)

사용자 지정 집합의 변수를 재설정하면 기본 집합에서 해당 변수의 현재 값으로 재설정되기만 합니다.

반대로, 기본 집합의 변수 값을 재설정하거나 변경하면 모든 사용자 지정 집합에서 해당 변수의 기본값이 항상 업데이트됩니다. 재설정 아이콘이 회색으로 비활성화된 경우, 이는 변수를 재설정할 수 없음을 나타내므로, 이는 해당 설정에서 변수에 사용자 정의된 값이 없음을 의미합니다. 사용자 지정 집합의 변수 값을 사용자 정의하지 않는 한, 기본 집합의 변수를 수정하면 변수 집합에 연결한 침입 정책에서 사용되는 값이 업데이트됩니다.

참고 변경 사항이 연결된 사용자 지정 집합의 변수를 사용하는 침입 정책에 영향을 미치는 방식을 평가하기 위해 기본 집합의 변수를 변경해 보는 것이 좋습니다. 사용자 지정 집합의 변수 값을 사용자 지정하지 않은 경우 특히 그렇습니다.

재설정 값을 보려면 변수 집합에서 재설정 아이콘 위에 마우스 포인터를 올려놓으면 됩니다. 사용자 지정 값과 재설정 값이 동일한 경우, 이는 다음 중 하나를 나타냅니다.

- 값 any로 변수를 추가한 맞춤형 또는 기본 집합에 있는 것임
- 고유한 값을 가진 변수를 추가하고 기본값으로 구성된 값을 사용하도록 선택한 사용자 지정 집합에 있는 것입니다

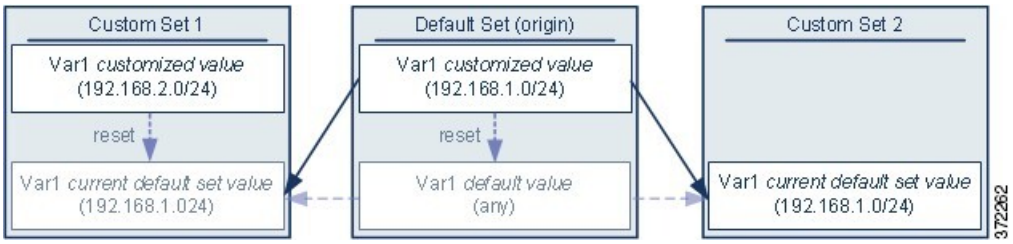
집합에 변수 추가

변수 집합에 변수를 추가하면 다른 모든 집합에 추가됩니다. 사용자 지정 집합에서 변수를 추가할 때 구성된 값을 기본 집합의 사용자 지정 값으로 사용할지 선택해야 합니다.

- 설정된 값**(**예**: 192.168.0.0/16)**을 사용하는 경우, 변수가 설정된 값을 기본값 any와 함께 사용자 지정 값으로 사용하는 기본 집합에 추가됩니다. 기본 집합의 현재 값이 다른 집합의 기본값을 결정하기 때문에, 다른 사용자 지정 집합의 초기 기본값은 구성된 값(예에서는 192.168.0.0/16)입니다.
- 설정된 값을 사용하지 않는 경우**,** 기본값 any만을 사용하여 변수가 기본 집합에 추가되므로 다른 사용자 지정 집합의 초기 기본값은 any가 됩니다.

예: 기본 집합에 사용자 정의 변수 추가

다음 다이어그램은 192.168.1.0/24 값이 있는 기본 집합에 사용자 정의 변수 Var1을 추가할 때의 집합 상호 작용에 대해 설명합니다.



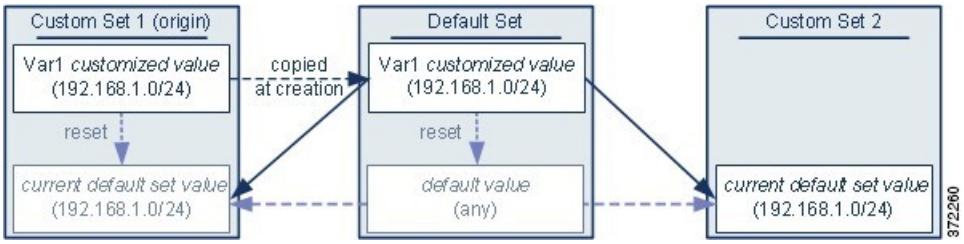
모든 집합에서 Var1 의 값을 사용자 지정할 수 있습니다. Var1이 사용자 정의되지 않은 사용자 지정 집합 2에서 해당 값은 192.168.1.0/24입니다. 사용자 지정 집합 1에서 Var1의 사용자 정의 값 192.168.2.0/24은 기본값을 오버라이드합니다. 기본 집합에서 사용자 정의 변수를 재설정하면 모든 집합에서 기본값을 any로 재설정합니다.

이 예에서 특히 주의해야 할 점은, 사용자가 Var1을 사용자 지정 집합 2에서 업데이트하지 않는 경우, 기본 집합에서 Var1을 사용자 지정하거나 재설정하면 결과적으로 사용자 지정 집합 2의 현재 Var1 기본값이 업데이트되며, 따라서 변수 집합에 연결된 모든 침입 규칙에 영향을 준다는 점입니다.

예에 표시되지 않지만 집합 간의 상호작용은 기본 집합의 기본 변수를 재설정하여 현재 규칙 업데이트에 의해 구성된 값을 재설정하지 않는 경우 사용자 정의 변수와 기본 변수에 대해 동일합니다.

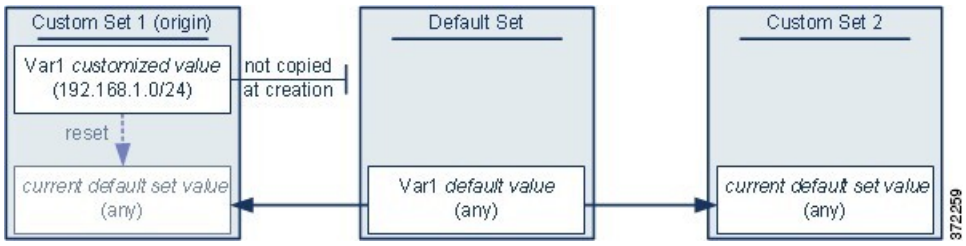
예: 맞춤형 집합에 사용자 정의 변수 추가

다음 두 가지 예는 사용자 정의 집합에 사용자 정의 변수를 추가할 때의 변수 집합 상호 작용에 대해 설명합니다. 새로운 변수를 저장할 때, 다른 집합에 대해 구성된 값을 기본값으로 사용하도록 설정할지 묻는 메시지가 표시됩니다. 다음 예에서, 구성된 값을 사용하도록 선택합니다.



사용자 지정 집합 1에서 Var1의 출처를 제외하고 이 예는 사용자가 기본 집합에 Var1을 추가한 위 예와 동일합니다. Var1에 대한 사용자 지정 값 192.168.1.0/24를 사용자 지정 집합 1에 추가하면 해당 값을 기본값 any와 함께 사용자 지정 값으로 기본 집합에 복사합니다. 따라서, Var1 값과 상호 작용은 사용자가 Var1을 기본 집합에 추가한 경우와 동일합니다. 이전 예와 마찬가지로, 기본 집합에서 Var1을 사용자 지정하거나 재설정하면 결과적으로 사용자 지정 집합 2의 현재 Var1 기본값이 업데이트되며, 따라서 변수 집합에 연결된 모든 침입 정책에 영향을 준다는 점에 유의하십시오.

다음 예에서는 이전 예처럼 값 192.168.1.0/24의 Var1을 Custom Set 1에 추가하되, Var1의 구성된 값을 다른 집합의 기본값으로 사용하지 않기로 선택합니다.



이 접근 방식은 `Var1`을 기본값 `any`를 가진 모든 집합에 추가합니다. `Var1`을 추가한 후 모든 집합의 값을 사용자 정의할 수 있습니다. 이 접근 방식의 이점은 기본 집합에서 `Var1`을 초기에 사용자 정의하지 않음으로써 기본 집합에서 값을 사용자 정의하여 `Var1`을 사용자 정의하지 않은 사용자 지정 집합 2와 같은 집합에서 현재 값을 부주의하게 변경하는 것의 위험을 줄일 수 있다는 것입니다.

중첩 변수

중첩 순환이 아닌 경우 변수를 중첩할 수 있습니다. 중첩된 부정 변수는 지원하지 않습니다.

유효한 중첩 변수

이 예에서는 SMTP_SERVERS, HTTP_SERVERS, OTHER_SERVERS가 유효한 중첩 변수입니다.

변수	유형	포함된 네트워크	제외된 네트워크
SMTP_SERVERS	사용자 지정 기본	10.1.1.1	—
HTTP_SERVERS	사용자 지정 기본	10.1.1.2	—
OTHER_SERVERS	사용자 정의	10.2.2.0/24	—
HOME_NET	사용자 지정 기본	10.1.1.0/24 OTHER_SERVERS	SMTP_SERVERS HTTP_SERVERS

유효하지 않은 중첩 변수

이 예에서는 HOME_NET의 중첩이 순환되므로 유효하지 않은 중첩 변수입니다. 즉 이는 HOME_NET을 포함한 OTHER_SERVERS을 정의하며 그 안에서 HOME_NET이 중첩됩니다.

변수	유형	포함된 네트워크	제외된 네트워크
SMTP_SERVERS	사용자 지정 기본	10.1.1.1	—
HTTP_SERVERS	사용자 지정 기본	10.1.1.2	—
OTHER_SERVERS	사용자 정의	10.2.2.0/24 HOME_NET	—

변수	유형	포함된 네트워크	제외된 네트워크
HOME_NET	사용자 지정 기본	10.1.1.0/24 OTHER_SERVERS	SMTP_SERVERS HTTP_SERVERS

지원되지 않는 중첩 부정 변수

중첩된 부정 변수는 지원되지 않기 때문에 이 예에서 보호된 네트워크 외부의 IP 주소를 나타내는 NONCORE_NET 변수를 사용할 수 없습니다.

변수	유형	포함된 네트워크	제외된 네트워크
HOME_NET	사용자 지정 기본	10.1.0.0/16 10.2.0.0/16 10.3.0.0/16	—
EXTERNAL_NET	사용자 지정 기본	—	HOME_NET
DMZ_NET	사용자 정의	10.4.0.0/16	—
NOT_DMZ_NET	사용자 정의	—	DMZ_NET
NONCORE_NET	사용자 정의	EXTERNAL_NET NOT_DMZ_NET	—

다른 지원되지 않는 중첩 부정 변수

위의 다른 예에서는 이 예에 표시된 대로 NONCORE_NET 변수를 생성해 보호된 네트워크 외부의 IP 주소를 표시할 수 있습니다.

변수	유형	포함된 네트워크	제외된 네트워크
HOME_NET	사용자 지정 기본	10.1.0.0/16 10.2.0.0/16 10.3.0.0/16	—
DMZ_NET	사용자 정의	10.4.0.0/16	—
NONCORE_NET	사용자 정의	—	HOME_NET DMZ_NET

변수 집합 관리

변수 집합을 사용하려면 위협 라이선스(threat defense 디바이스용) 또는 보호 라이선스(기타 모든 디바이스 유형)가 있어야 합니다.

다중 도메인 구축에서 시스템은 현재 도메인에서 생성된 개체를 표시하며 이러한 개체는 수정할 수 있습니다. 상위 도메인에서 생성된 개체도 표시되지만, 이러한 개체는 수정할 수 없습니다. 하위 도메인에서 생성된 개체를 보고 수정하려면 해당 도메인으로 전환하십시오.

프로시저

단계 **1** **Objects(**개체**)** > **Object Management(**개체 관리**)**을(를) 선택합니다.

단계 **2** 개체 유형 목록에서 **Variable Set(**변수 집합**)**을 선택합니다.

단계 **3** 변수 세트 관리:

- 추가 - 사용자 정의 변수 집합을 추가하려면 **Add Variable Set(**변수 집합 추가**)**를 클릭합니다. 변수 집합 생성, 107 페이지를 참조하십시오.
- 삭제 - 사용자 지정 변수 집합을 삭제하려면 변수 집합 옆의 **Delete(**삭제**)** ( )을 클릭하고 예를 클릭합니다. 기본 변수 집합 또는 상위 도메인에 속한 변수 집합을 삭제할 수 없습니다.

  참고 삭제한 변수 집합에서 생성된 변수는 삭제되거나 다른 집합에 영향을 받지 않습니다.

- 편집 - 변수 세트를 편집하려면 수정하려는 변수 집합 옆의 **Edit(**수정**)** ( )을 클릭합니다. 개체 수정, 7 페이지의 내용을 참조하십시오.
- 필터 - 이름으로 변수 집합을 필터링하려면 이름을 입력합니다. 입력하는 동안 페이지가 새로 고침되며 일치하는 이름을 표시합니다. 이름 필터링을 삭제하고 싶은 경우 필터 필드의 **Clear(**지우기**)** ( )을 클릭합니다.
- 변수 관리 - 변수 집합에 포함된 변수를 관리하려면 변수 관리, 108 페이지의 내용을 참조하십시오.

변수 집합 생성

프로시저

단계 **1** **Objects(**개체**)** > **Object Management(**개체 관리**)**을(를) 선택합니다.

단계 **2** 개체 유형 목록에서 **Variable Set(**변수 집합**)**을 선택합니다.

단계 **3** **Add Variable Set(**변수 집합 추가**)**를 클릭합니다.

단계 **4** **Name(**이름**)**을 입력합니다.

다중 도메인 구축에서 개체 이름은 도메인 계층 내에서 고유해야 합니다. 시스템은 현재 도메인에서 확인할 수 없는 개체 이름과의 충돌을 식별할 수 있습니다.

단계 **5** 필요한 경우 **Description(**설명**)**을 입력합니다.

단계 **6** 집합의 변수를 관리하려면 변수 관리, 108 페이지의 내용을 참조하십시오.

단계 **7** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

- 활성 정책이 개체를 참조하는 경우 구성 변경 사항을 구축합니다. 참조.

변수 관리

위협 라이선스(threat defense 디바이스용) 또는 보호 라이선스(기타 모든 디바이스 유형)가 있어야 합니다.

다중 도메인 구축에서 시스템은 현재 도메인에서 생성된 개체를 표시하며 이러한 개체는 수정할 수 있습니다. 상위 도메인에서 생성된 개체도 표시되지만, 이러한 개체는 수정할 수 없습니다. 하위 도메인에서 생성된 개체를 보고 수정하려면 해당 도메인으로 전환하십시오.

프로시저

단계 **1** **Objects(**개체**)** > **Object Management(**개체 관리**)**을(를) 선택합니다.

단계 **2** 개체 유형 목록에서 **Variable Set(**변수 집합**)**을 선택합니다.

단계 **3** 편집하려는 변수 집합 옆에 있는 **Edit(**수정**)** ( )을 클릭합니다.

View(보기**)** ( )이 대신 표시되는 경우에는 설정이 상위 도메인에 속하거나 설정을 수정할 권한이 없는 것입니다.

단계 **4** 변수 관리

- 표시 - 변수에 대한 완전한 값을 표시하려는 경우 변수 옆 값 열의 값 위로 마우스를 이동합니다.
- 추가 - 변수를 추가하려면 **Add(**추가**)**를 클릭합니다. 변수 추가, 109 페이지를 참조하십시오.
- 삭제 - 변수 옆의 **Delete(**삭제**)** ( )를 클릭합니다. 변수를 추가한 뒤 변수 집합을 저장한 경우 변수를 삭제하려면 **Yes(**예**)**를 클릭합니다.

  다음은 삭제가 불가능합니다.

  - 기본 변수
  - 침입 규칙 또는 다른 변수에서 사용되는 사용자 정의 변수
  - 상위 도메인에 속하는 변수

- 편집 - 편집하려는 변수 옆에 있는 **Edit(**수정**)** ( )을 클릭합니다. 변수 편집, 110 페이지의 내용을 참조하십시오.
- 재설정 - 수정된 변수를 기본값으로 재설정하려는 경우, 수정된 변수 옆의 **Reset(**재설정**)**을 클릭합니다. 재설정 아이콘이 흐리게 표시되는 경우, 다음 중 하나에 해당합니다.

- 현재 값은 이미 기본 값입니다.
- 설정이 상위 도메인에 속합니다.

팁 기본값을 표시하려면 활성 재설정 위에 마우스 포인터를 올려놓습니다.

단계 **5** 변수 집합을 저장하려면 **Save(**저장**)**을 클릭합니다. 변수 집합이 액세스 제어 정책에서 사용 중인 경우 변경 사항을 저장하려면 **Yes(**예**)**를 클릭합니다.

기본 집합의 현재 값이 다른 모든 집합의 기본값을 결정하기 때문에 기본 집합의 변수를 수정하거나 재설정하면 기본값을 사용자 정의하지 않은 집합에서 현재 값이 변경됩니다.

다음에 수행할 작업

- 활성 정책이 개체를 참조하는 경우 구성 변경 사항을 구축합니다. 참조.

변수 추가

위협 라이선스(threat defense 디바이스용) 또는 보호 라이선스(기타 모든 디바이스 유형)가 있어야 합니다.

프로시저

단계 **1** 변수 집합 편집기에서 **Add(**추가**)**를 클릭합니다.

단계 **2** 고유한 변수 **Name(**이름**)**을 입력합니다.

단계 **3** **Type(**유형**)** 드롭다운 목록에서 **Network(**네트워크**)** 또는 **Port(**포트**)**를 선택합니다.

단계 **4** 변수 값을 지정합니다.

- 사용 가능한 네트워크 또는 포트 목록에서 항목을 포함 또는 제외 항목으로 이동하려면 하나 이상의 항목을 선택하고 드래그앤드롭을 사용하거나 **Include(**포함**)** 또는 **Exclude(**제외**)**를 클릭합니다.

  팁 네트워크 또는 포트 변수에 대해 포함되거나 제외된 목록에서 주소 또는 포트가 중복되는 경우, 제외된 주소 또는 포트가 우선합니다.

- 단일 리터럴 값을 입력한 다음 **Add(**추가**)**를 클릭합니다. 네트워크 변수에 대해, 단일 IP 주소 또는 주소 블록을 입력할 수 있습니다. 포트 변수의 경우 단일 포트 또는 포트 범위를 추가할 수 있는데, 하이픈(-)으로 높은 값과 낮은 값을 나눕니다. 여러 문자 값을 입력하기 위해 필요한 만큼 이 단계를 반복합니다.
- 포함되거나 제외된 목록에서 항목을 제거하려면 항목 옆의 **Delete(**삭제**)** ( )를 클릭합니다.

참고 포함 또는 제외할 항목 목록은 리터럴 문자열 및 기존 변수, 개체, 네트워크 변수일 경우 네트워크 개체 그룹의 모든 조합으로 구성될 수 있습니다.

단계 **5** **Save(**저장**)**을 클릭하여 변수를 저장합니다. 사용자 지정 집합에서 새로운 변수를 추가하는 경우 다음과 같은 옵션을 사용할 수 있습니다.

- 구성된 값을 기본 집합의 맞춤화된 값으로 사용하는 변수를 추가하여 다른 맞춤형 집합의 기본값이 되도록 하려면 **Yes(**예**)**를 클릭합니다.
- 변수를 기본 집합 및 다른 사용자 정의 집합에 `Any(모든)` 기본값으로 추가하려면 **No(**아니오**)**를 클릭합니다.

단계 **6** 변수 집합을 저장하려면 **Save(**저장**)**을 클릭합니다. 변경 사항이 저장되며 변수 집합이 연결된 모든 액세스 제어 정책이 오래된 상태로 표시됩니다.

다음에 수행할 작업

- 활성 정책이 개체를 참조하는 경우 구성 변경 사항을 구축합니다. 참조.

변수 편집

위협 라이선스(threat defense 디바이스용) 또는 보호 라이선스(기타 모든 디바이스 유형)가 있어야 합니다.

다중 도메인 구축에서 시스템은 현재 도메인에서 생성된 개체를 표시하며 이러한 개체는 수정할 수 있습니다. 상위 도메인에서 생성된 개체도 표시되지만, 이러한 개체는 수정할 수 없습니다. 하위 도메인에서 생성된 개체를 보고 수정하려면 해당 도메인으로 전환하십시오.

사용자 정의 및 기본 변수를 편집할 수 있습니다.

기존 변수의 이름 또는 유형을 변경할 수 없습니다.

프로시저

단계 **1** 변수 집합 편집기에서 수정하려는 변수 옆의 **Edit(**수정**)** ( )을 클릭합니다.

View(보기**)** ( )가 대신 표시되는 경우에는 개체가 상위 도메인에 속하거나 개체를 수정할 권한이 없는 것입니다.

단계 **2** 변수를 수정합니다.

- 사용 가능한 네트워크 또는 포트 목록에서 항목을 포함 또는 제외 항목으로 이동하려면 하나 이상의 항목을 선택하고 드래그앤드롭을 사용하거나 **Include(**포함**)** 또는 **Exclude(**제외**)**를 클릭합니다.

  팁 네트워크 또는 포트 변수에 대해 포함되거나 제외된 목록에서 주소 또는 포트가 중복되는 경우, 제외된 주소 또는 포트가 우선합니다.

- 단일 리터럴 값을 입력한 다음 **Add(**추가**)**를 클릭합니다. 네트워크 변수에 대해, 단일 IP 주소 또는 주소 블록을 입력할 수 있습니다. 포트 변수의 경우 단일 포트 또는 포트 범위를 추가할 수 있

는데, 하이픈(-)으로 높은 값과 낮은 값을 나눕니다. 여러 문자 값을 입력하기 위해 필요한 만큼 이 단계를 반복합니다.

- 포함되거나 제외된 목록에서 항목을 제거하려면 항목 옆의 **Delete(**삭제**)** ( )를 클릭합니다.

참고 포함 또는 제외할 항목 목록은 리터럴 문자열 및 기존 변수, 개체, 네트워크 변수일 경우 네트워크 개체 그룹의 모든 조합으로 구성될 수 있습니다.

단계 **3** **Save(**저장**)**을 클릭하여 변수를 저장합니다.

단계 **4** 변수 집합을 저장하려면 **Save(**저장**)**을 클릭합니다. 변수 집합이 액세스 제어 정책에서 사용 중인 경우 변경 사항을 저장하려면 **Yes(**예**)**를 클릭합니다. 변경 사항이 저장되며 변수 집합이 연결된 모든 액세스 제어 정책이 오래된 상태로 표시됩니다.

다음에 수행할 작업

- 활성 정책이 개체를 참조하는 경우 구성 변경 사항을 구축합니다. 참조.

VLAN Tag

구성하는 각 VLAN 태그 객체는 VLAN 태그 또는 태그 범위를 나타냅니다.

VLAN 태그 개체를 그룹화할 수 있습니다. 그룹은 여러 개체를 나타냅니다. 단일 개체의 VLAN 태그 범위를 사용하는 것은 그룹으로 간주되지 않습니다.

규칙 및 이벤트 검색을 포함해 시스템 웹 인터페이스의 여러 위치에서 VLAN 태그 개체 및 그룹을 사용할 수 있습니다. 예를 들어 특정 VLAN에만 적용되는 액세스 제어 규칙을 작성할 수 있습니다.

VLAN 태그 개체 생성

프로시저

단계 **1** **Objects(**개체**)** > **Object Management(**개체 관리**)**을(를) 선택합니다.

단계 **2** 개체 유형 목록에서 **VLAN tag(VLAN** 태그**)**를 선택합니다.

단계 **3** 드롭다운 목록의 **Add VLAN tag(VLAN** 태그 추가**)**에서 **Add Object(**개체 추가**)**를 선택합니다.

단계 **4** **Name(**이름**)**을 입력합니다.

단계 **5** **Description(**설명**)**을 입력합니다.

단계 **6** **VLAN** 태그 필드에 값을 입력합니다. VLAN 태그의 범위를 지정하려면 하이픈을 사용합니다.

단계 **7** 개체에 대한 재정의를 관리합니다.

- 이 개체에 대한 재정의를 허용하려면 **Allow Overrides(**재정의 허용**)** 확인란을 선택합니다. 개체 재정의 허용, 13 페이지의 내용을 참조하십시오.

- 이 개체에 재정의 값을 추가하려면 Override(재정의) 섹션을 펼치고 **Add(**추가**)**를 클릭합니다. 개체 재정의 추가, 14 페이지의 내용을 참조하십시오.

단계 **8** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

- 활성 정책이 개체를 참조하는 경우 구성 변경 사항을 구축합니다. 참조.

VPN

threat defense 디바이스에서 다음 VPN 개체를 사용할 수 있습니다. 이러한 개체를 사용하려면 관리자 권한이 있어야 하며, 스마트 라이선스 계정이 내보내기 제어를 충족해야 합니다. 이러한 개체는 리프 도메인에서만 설정할 수 있습니다.

Threat Defense IKE 정책

IKE(Internet Key Exchange)는 IPsec 피어를 인증하고, IPsec 암호화 키를 협상 및 배포하고, IPsec SA(보안 연계)를 자동으로 설정하는 데 사용되는 키 관리 프로토콜입니다. IKE 협상은 2단계로 구성됩니다. 1단계에서는 두 IKE 피어 간의 보안 연계를 협상합니다. 그러면 피어가 2단계에서 안전하게 통신할 수 있습니다. 2단계 협상 중에는 IKE가 IPsec 등의 기타 애플리케이션에 대해 SA를 설정합니다. 두 단계에서는 모두 연결을 협상할 때 제안을 사용합니다. IKE 제안은 두 피어가 상호 간의 IKE 협상을 보호하는 데 사용하는 알고리즘 집합입니다. IKE 협상에서는 두 피어가 먼저 공통(공유) IKE 정책을 합의합니다. 이 정책은 후속 IKE 협상을 보호하는 데 사용되는 보안 파라미터를 제시합니다.

IKEv1의 경우, IKE 제안에는 단일 알고리즘 집합과 모듈러스 그룹이 포함됩니다. 적어도 하나 이상의 정책이 원격 피어의 정책과 일치하도록 우선 순위가 지정된 여러 정책을 생성할 수 있습니다. IKEv1과는 달리 IKEv2 제안의 경우, 한 그룹에서 여러 알고리즘과 모듈러스 그룹을 선택할 수 있습니다. 피어가 1단계 협상 중에 선택하기 때문에 단일 IKE 제안을 생성할 수 있도록 하지만 가장 원하는 옵션에 더 높은 우선 순위를 부여하는 여러 다른 제안을 고려하십시오. IKEv2의 경우 정책 개체가 인증을 지정하지 않으면 다른 정책이 인증 요건을 정의해야 합니다.

사이트 대 사이트 IPsec VPN을 구성할 때 IKE 정책이 필요합니다. 자세한 내용은 VPN를 참고하십시오.

IKEv1 정책 개체 구성

IKEv1 정책 페이지를 사용하여 IKEv1 정책 개체를 생성, 삭제, 편집합니다. 이러한 정책 개체는 IKEv1 정책에 필요한 파라미터를 포함합니다.

프로시저

단계 **1** 개체 > 개체 관리를 선택하고 목차에서 **VPN** > **IKEv1** 정책을 선택합니다.

이전에 구성된 정책이 시스템이 정의한 기본값을 포함하여 나열됩니다. 액세스 수준에 따라 제안을 **Edit(**수정**)** ( )하거나 보거나(**View(**보기**)** ( )) **Delete(**삭제**)** ( )할 수 있습니다.

단계 **2** (선택 사항) **Add(**추가**)** ( )**Add IKEv1 Policy(IKEv1** 정책 추가**)**를 선택해 새 정책 개체를 만들 수 있습니다.

단계 **3** 이 정책의 이름을 입력합니다. 최대 128자를 입력할 수 있습니다.

단계 **4** (선택 사항) 이 제안의 설명을 입력하십시오. 최대 1,024자를 입력할 수 있습니다.

단계 **5** IKE 정책의 우선 순위 값을 입력합니다.

우선 순위에 따라 일반 SA(보안 연계) 찾기를 시도할 때 두 협상 피어가 비교하는 IKE 정책의 순서가 결정됩니다. 원격 IPsec 피어가 최고 우선 순위 정책에서 선택한 파라미터를 지원하지 않는 경우 그 다음 우선 순위에 정의된 파라미터 사용을 시도합니다. 유효한 값의 범위는 1~65535입니다. 번호가 낮을수록 우선 순위가 높습니다. 이 필드를 공백으로 두면 Management Center는 1, 5 순으로 5씩 증가시키며 할당되지 않은 가장 낮은 값을 할당합니다

단계 **6** **Encryption(**암호화**)** 방법을 선택합니다.

IKEv1 정책에 사용할 암호화 및 해시 알고리즘을 정의할 때 피어 디바이스가 지원하는 알고리즘으로 선택이 제한됩니다. VPN 토폴로지의 엑스트라넷 디바이스의 경우 두 피어 모두 일치하는 알고리즘을 선택해야 합니다. IKEv1의 경우 다음 옵션 중 하나를 선택합니다. 옵션에 대한 자세한 설명은 사용할 암호화 알고리즘 결정를 참조하십시오.

단계 **7** 메시지 무결성을 보장하는 데 사용되는 메시지 다이제스트를 생성하는 해시 알고리즘을 선택합니다.

IKEv1 제안에 사용할 암호화 및 해시 알고리즘을 정의할 때 관리되는 디바이스가 지원하는 알고리즘으로 선택이 제한됩니다. VPN 토폴로지의 엑스트라넷 디바이스의 경우 두 피어 모두 일치하는 알고리즘을 선택해야 합니다. 옵션에 대한 자세한 설명은 사용할 해시 알고리즘 결정를 참조하십시오.

단계 **8** **Diffie-Hellman** 그룹을 설정합니다.

Diffie-Hellman 그룹은 암호화에 사용됩니다. 대형 모듈러스는 보안성은 더 높지만, 처리 시간이 더 오래 걸립니다. 두 피어의 모듈러스 그룹이 일치해야 합니다. VPN에서 허용하려면 그룹을 선택합니다. 옵션에 대한 자세한 설명은 사용할 Diffie-Hellman 모듈러스 그룹 결정를 참조하십시오.

단계 **9** 보안 연결(SA)의 수명을 초 단위로 설정합니다. 120~2147483647초 사이의 값을 지정할 수 있습니다. 기본값은 86400입니다.

라이프타임이 초과되면 SA는 만료되며 두 피어 간에 SA를 재협상해야 합니다. 일반적으로 (특정 지점까지는) 수명이 짧을수록 IKE 협상이 보다 안전합니다. 그러나 라이프타임이 길면 라이프타임이 짧은 경우에 비해 이후 IPsec 보안 연계를 더 빠르게 설정할 수 있습니다.

단계 **10** 두 피어 간에 사용할 인증 방법을 선택합니다.

- 사전 공유 키 - 사전 공유 키를 사용하면 두 피어 간 보안 키를 공유할 수 있으며 인증 단계에서 IKE가 사용할 수 있습니다. 피어에 구성된 피어 중 하나가 동일한 사전 공유 키로 구성되지 않은 경우 IKE SA를 설정할 수 없습니다.
- 인증서 - VPN 연결 인증 방법으로 인증서를 사용하는 경우 피어는 인증을 위해 PKI 인프라의 CA 서버에서 디지털 인증서를 가져와 거래합니다.

참고 IKEv1을 지원하는 VPN 토폴로지에서는 선택한 IKEv1 정책 개체에서 지정된 **Authentication Method(**인증 방법**)**가 IKEv1 **Authentication Type(**인증 유형**)** 설정의 기본값이 됩니다. 이러한 값은 서로 일치해야 하며, 그렇지 않을 경우 컨피그레이션에 오류가 발생합니다.

단계 **11** **Save(**저장**)**를 클릭합니다.
새 IKEv1 정책이 목록에 추가됩니다.

IKEv2 정책 개체 구성

IKEv2 정책 대화 상자를 사용하여 IKEv2 정책 개체를 생성, 삭제, 편집합니다. 이러한 정책 개체는 IKEv2 정책에 필요한 파라미터를 포함합니다.

프로시저

단계 **1** 개체 > 개체 관리를 선택하고 목차에서 **VPN** > **IKEv2** 정책을 선택합니다.

이전에 구성된 정책이 시스템이 정의한 기본값을 포함하여 나열됩니다. 액세스 수준에 따라 정책을 **Edit(**수정**)** ( ), **View(**보기**)** ( ), **Delete(**삭제**)** ( )할 수 있습니다.

단계 **2** **Add(**추가**)** ( )**Add IKEv2 Policy(IKEv2** 정책 추가**)**를 선택해 새 정책을 생성합니다.

단계 **3** 이 정책의 이름을 입력합니다.

정책 개체의 이름입니다. 최대 128자를 입력할 수 있습니다.

단계 **4** 이 정책에 대한 설명을 입력합니다.

정책 개체의 설명입니다. 최대 1024자를 입력할 수 있습니다.

단계 **5** 우선 순위를 입력합니다.

IKE 제안의 우선 순위 값입니다. 우선 순위에 따라 일반 SA(보안 연계) 찾기를 시도할 때 두 협상 피어가 비교하는 IKE 제안의 순서가 결정됩니다. 원격 IPsec 피어가 최고 우선 순위 정책에서 선택한 파라미터를 지원하지 않는 경우 그 다음 우선 순위에 정의된 파라미터 사용을 시도합니다. 유효한 값의 범위는 1~65535입니다. 번호가 낮을수록 우선 순위가 높습니다. 이 필드를 공백으로 두면 Management Center는 1, 5 순으로 5씩 증가시키며 할당되지 않은 가장 낮은 값을 할당합니다

단계 **6** 보안 연결(SA)의 수명을 초 단위로 설정합니다. 120~2147483647초 사이의 값을 지정할 수 있습니다. 기본값은 86400입니다.

라이프타임이 초과되면 SA는 만료되며 두 피어 간에 SA를 재협상해야 합니다. 일반적으로 (특정 지점까지는) 수명이 짧을수록 IKE 협상이 보다 안전합니다. 그러나 라이프타임이 길면 라이프타임이 짧은 경우에 비해 이후 IPsec 보안 연계를 더 빠르게 설정할 수 있습니다.

단계 **7** IKE 정책에 사용되는 해시 알고리즘의 무결성 알고리즘 부분을 선택합니다. 메시지 무결성을 보장하는 데 사용되는 메시지 다이제스트를 생성하는 해시 알고리즘을 선택합니다.

IKEv2 제안에 사용할 암호화 및 해시 알고리즘을 정의할 때 관리되는 디바이스가 지원하는 알고리즘으로 선택이 제한됩니다. VPN 토폴로지의 엑스트라넷 디바이스를 위해 두 피어 모두 일치하는 알고리즘을 선택해야 합니다. VPN에서 허용하려는 모든 알고리즘을 선택합니다.옵션에 대한 자세한 설명은 사용할 해시 알고리즘 결정를 참조하십시오.

단계 **8** 2단계 협상 보호를 위한 1단계 SA를 설정하는 데 사용되는 암호화 알고리즘을 선택합니다.

IKEv2 제안에 사용할 암호화 및 해시 알고리즘을 정의할 때 관리되는 디바이스가 지원하는 알고리즘으로 선택이 제한됩니다. VPN 토폴로지의 엑스트라넷 디바이스를 위해 두 피어 모두 일치하는 알고리즘을 선택해야 합니다. VPN에서 허용하려는 모든 알고리즘을 선택합니다. 옵션에 대한 자세한 설명은 사용할 암호화 알고리즘 결정를 참조하십시오.

단계 **9** **PRF** 알고리즘을 선택합니다.

IKE 정책에 사용되는 해시 알고리즘의 의사 난수 함수(PRF) 부분입니다. IKEv1에서는 무결성 및 PRF 알고리즘이 구분되지 않지만 IKEv2에서는 이러한 요소에 대해 서로 다른 알고리즘을 지정할 수 있습니다. VPN에서 허용하려는 모든 알고리즘을 선택합니다. 옵션에 대한 자세한 설명은 사용할 해시 알고리즘 결정를 참조하십시오.

단계 **10** **DH** 그룹을 선택하고 추가합니다.

Diffie-Hellman 그룹은 암호화에 사용됩니다. 대형 모듈러스는 보안성은 더 높지만, 처리 시간이 더 오래 걸립니다. 두 피어의 모듈러스 그룹이 일치해야 합니다. VPN에서 허용할 그룹을 선택합니다. 옵션에 대한 자세한 설명은 사용할 Diffie-Hellman 모듈러스 그룹 결정를 참조하십시오.

단계 **11** **Save(**저장**)**를 클릭합니다.
유효한 선택 조합이 선택된 경우 새 IKEv2 정책이 목록에 추가됩니다. 그렇지 않으면 오류가 표시되며 정책을 성공적으로 저장하기 위해 변경해야 합니다.

Threat Defense IPSec 제안

IPsec 제안(또는 변형 집합)은 VPN 토폴로지를 구성할 때 사용됩니다. ISAKMP와의 IPsec 보안 연계 협상에서 피어는 특정 데이터 흐름을 보호하기 위해 특정 제안을 사용하는 데 동의합니다. 제안은 두 피어 모두에 동일해야 합니다.

IKE 버전(IKEv1 또는 IKEv2)에 따라 각기 다른 IPsec 제안 개체가 있습니다.

- IKEv1 IPsec 제안(변형 집합)을 생성할 때는 IPsec가 동작하는 모드를 선택하고 필요한 암호화 및 인증 유형을 정의합니다. 알고리즘에 대해서는 단일 옵션을 선택할 수 있습니다. VPN에서 여러 조합을 지원하려면 여러 IKEv1 IPsec 제안 개체를 생성합니다.
- IKEv2 IPsec 제안 개체를 생성할 때는 VPN에서 허용되는 모든 암호화 및 해시 알고리즘을 선택할 수 있습니다. IKEv2 협상 중에 피어는 서로 도움이 되는 가장 적절한 옵션을 선택합니다.

IKEv1 및 IKEv2 IPsec 제안에는 모두 ESP(Encapsulating Security Protocol)가 사용됩니다. ESP는 인증, 암호화 및 재생 방지 서비스를 제공합니다. ESP는 IP 프로토콜 유형 50입니다.

참고 IPsec 터널에서는 암호화 및 인증을 모두 사용하는 것이 좋습니다.

IKEv1 IPsec 제안 개체 설정

프로시저

단계 1 개체 > 개체 관리를 선택하고 목차에서 **VPN** > **IPsec IKev1** 제안을 선택합니다.

이전에 구성된 제안이 시스템이 정의한 기본값을 포함하여 나열됩니다. 액세스 수준에 따라 제안을 **Edit(**수정**)** ( )하거나 보거나(**View(**보기**)** ( )) **Delete(**삭제**)** ( )할 수 있습니다.

단계 2 **Add(**추가**)** ( )**Add IPsec IKEv1 Proposal(IPsec IKEv1** 제안 추가**)**를 선택하여 새 제안을 만들 수 있습니다.

단계 3 이 제안의 이름을 입력합니다.

정책 개체의 이름입니다. 최대 128자를 입력할 수 있습니다.

단계 4 이 제안의 설명을 입력하십시오.

정책 개체의 설명입니다. 최대 1024자를 입력할 수 있습니다.

단계 5 **ESP** 암호화 방법을 선택합니다. 이 제안에 대한 ESP(Encapsulating Security Protocol) 암호화 알고리즘입니다.

IKEv1의 경우 다음 옵션 중 하나를 선택합니다. IPsec 제안에 사용할 암호화 및 해시 알고리즘을 결정할 때는 VPN의 디바이스가 지원하는 알고리즘으로 선택이 제한됩니다. 옵션에 대한 자세한 설명은 사용할 암호화 알고리즘 결정를 참조하십시오.

단계 6 **ESP** 해시에 대한 옵션을 선택합니다.

옵션에 대한 자세한 설명은 사용할 해시 알고리즘 결정를 참조하십시오.

단계 7 **Save(**저장**)**를 클릭합니다.
새 제안이 목록에 추가됩니다.

IKEv2 IPsec 제안 개체 설정

프로시저

단계 1 **Objects(**개체**)** > **Object Management(**개체 관리**)**를 선택하고 목차에서 **VPN** > **IKev2 IPsec** 제안**(IKEv2 IPsec Proposal)**을 선택합니다.

이전에 구성된 제안이 시스템이 정의한 기본값을 포함하여 나열됩니다. 액세스 수준에 따라 제안을 편집(**Edit(**수정**)** (✎)), 보기(**View(**보기**)** (👁)), 삭제(**Delete(**삭제**)** (🗑))할 수 있습니다.

단계 **2** **Add(**추가**)** (＋)**Add IPsec IKEv2 Proposal(IPsec IKEv2** 제안 추가**)**를 선택하여 새 제안을 만들 수 있습니다.

단계 **3** 이 제안의 이름을 입력합니다.

정책 개체의 이름입니다. 최대 128자를 입력할 수 있습니다.

단계 **4** 이 제안의 설명을 입력하십시오.

정책 개체의 설명입니다. 최대 1024자를 입력할 수 있습니다.

단계 **5** 인증에 대한 제안에 사용되는 해시 또는 무결성 알고리즘인 **ESP** 해시 방법을 선택합니다.

참고 Threat Defense NULL 암호화를 사용하는 IPSec 터널을 지원하지 않습니다. IPSec IKEv2 제안에 대해 NULL 암호화를 선택하지 않아야 합니다.

IKEv2의 경우 **ESP** 해시를 지원하려는 모든 옵션을 선택합니다. 옵션에 대한 자세한 설명은 사용할 해시 알고리즘 결정를 참조하십시오.

단계 **6** **ESP** 암호화 방법을 선택합니다. 이 제안에 대한 ESP(Encapsulating Security Protocol) 암호화 알고리즘입니다.

IKEv2의 경우 선택을 클릭하여 지원하려는 모든 옵션을 선택할 수 있는 대화 상자를 엽니다. IPsec 제안에 사용할 암호화 및 해시 알고리즘을 결정할 때는 VPN의 디바이스가 지원하는 알고리즘으로 선택이 제한됩니다. 옵션에 대한 자세한 설명은 사용할 암호화 알고리즘 결정를 참조하십시오.

단계 **7** **Save(**저장**)**를 클릭합니다.
새 제안이 목록에 추가됩니다.

Threat Defense 그룹 정책 개체

그룹 정책은 원격 액세스 VPN 경험을 정의하는 그룹 정책 개체가 저장된 속성 및 값 쌍의 집합입니다. 예를 들어 그룹 정책 개체에서는 주소, 프로토콜, 연결 설정 등 일반 속성을 구성합니다.

VPN 터널이 설정된 경우 사용자에게 적용되는 그룹 정책이 결정됩니다. RADIUS 권한 서버는 그룹 정책을 할당하거나 현재 연결 프로파일에서 그룹 정책을 가져옵니다.

참고 threat defense에 그룹 정책 속성 상속이 없습니다. 그룹 정책 개체 전체가 사용자에 대해 사용됩니다. 로그인 시 AAA 서버에서 식별된 그룹 정책 개체가 사용됩니다. 이를 지정하지 않은 경우, VPN 연결을 위해 구성된 기본 그룹 정책이 사용됩니다. 제공된 기본 그룹 정책은 기본값으로 설정할 수 있으나, 해당 정책이 연결 프로파일에 할당되어 있고 사용자의 다른 그룹 정책이 식별되지 않은 경우에만 사용됩니다.

그룹 개체를 사용하려면 Export Controlled Features(내보내기 제어 기능)가 있는 Smart License(스마트 라이선스) 계정과 연결된 이러한 AnyConnect Client 라이선스 중 하나를 활성화해야 합니다.

- AnyConnect VPN Only
- AnyConnect Plus
- AnyConnect Apex

관련 항목

그룹 정책 개체 설정, 118 페이지

그룹 정책 개체 설정

Threat Defense 그룹 정책 개체, 117 페이지의 내용을 참조하십시오.

프로시저

단계 **1** **Objects(**개체**)** > **Object Management(**개체 관리**)** > **VPN** > **Group Policy(**그룹 정책**)**을 선택합니다.

이전에 구성된 정책이 시스템 기본값을 포함하여 나열됩니다. 액세스 수준에 따라 편집, 보기 또는 그룹 정책 삭제를 할 수 있습니다.

단계 **2** **Add Group Policy(**그룹 정책 추가**)**를 클릭하거나 현재 정책을 선택하여 편집합니다.

단계 **3** 이 정책의 이름을 입력하고 필요한 경우 설명을 입력합니다.

이름은 최대 64자까지 입력할 수 있고 공백이 허용됩니다. 설명은 최대 1,024자까지 입력할 수 있습니다.

단계 **4** 그룹 정책에 그룹 정책 일반 옵션, 119 페이지에 설명된 **General(**일반**)** 파라미터를 지정합니다.

단계 **5** 그룹 정책 AnyConnect Client 옵션, 121 페이지에 설명된 대로 이 그룹 정책에 대한 **AnyConnect** 매개변수를 지정합니다.

단계 **6** 그룹 정책에 그룹 정책 고급 옵션, 125 페이지에 설명된 **Advanced(**고급**)** 파라미터를 지정합니다.

단계 **7** **Save(**저장**)**를 클릭합니다.
새 그룹 정책이 목록에 추가됩니다.

다음에 수행할 작업

그룹 정책 개체를 원격 액세스 VPN 연결 프로파일에 추가합니다.

그룹 정책 일반 옵션

탐색 경로

Objects(개체**)** > **Object Management(**개체 관리**)** > **VPN** > **Group Policy(**그룹 정책**)**는 **Add Group Policy(**그룹 정책 추가**)**를 클릭하거나 현재 정책을 선택하여 편집합니다.을 클릭하고 **General(**일반**)** 탭을 선택합니다.

VPN 프로토콜 필드

이 그룹 정책을 적용할 때 사용할 수 있는 원격 액세스 VPN 터널 유형을 지정합니다. **SSL** 또는 **IPsec IKEv2**.

IP 주소 풀

원격 액세스 VPN에서 사용자 그룹에 특정된 주소 풀을 기준으로 적용되는 IPv4 주소 할당을 지정합니다. 원격 액세스 VPN의 경우 인증에 RADIUS/ISE를 사용해 식별된 사용자 그룹에 대한 특정 주소 풀에서 IP 주소를 할당할 수 있습니다. 특정 사용자 그룹에 대한 RADIUS 인증 속성(GroupPolicy/Class)으로 특정 사용자 그룹 정책을 구성하여 ID가 인식되지 않은 시스템에서 사용자 또는 사용자 그룹에 대한 정책을 원활하게 적용할 수 있습니다. 예를 들어 해당 주소를 사용하는 계약자 및 정책 시행이 내부 네트워크에 제한된 액세스를 허용하도록 특정 주소 풀을 선택해야 합니다.

IPv4 주소 풀을 클라이언트에 할당하는 threat defense 디바이스의 환경설정 순서

1. IPv4Address 풀에 대한 RADIUS 특성
2. 그룹 정책에 대한 RADIUS 특성
3. 연결 프로파일에 매핑된 그룹 정책의 주소 풀
4. 연결 프로파일의 IPv4Address 풀

그룹 정책의 IP 주소 풀을 사용할 때 몇 가지 제한 사항:

- IPv6 주소 풀은 지원되지 않습니다.
- 그룹 정책에서 최대 6개의 IPv4 주소 풀을 구성할 수 있습니다.
- 사용 중인 주소 풀이 수정되는 경우 구축 실패로 표시됩니다. 주소 풀을 변경하기 전에 모든 사용자를 로그오프해야 합니다.
- 주소 풀의 이름이 변경되거나 겹치는 주소 풀이 구성되면 구축을 실패할 수 있습니다. 기존 주소 풀을 제허아고 변경된 주소 풀을 재구축하여 변경 사항을 구축해야 합니다.

  일부 문제 해결 명령:

  - `show ip local pool <address-pool-name>`
  - `show vpn-sessiondb detail anyconnect`
  - `vpn-sessiondb loggoff all noconfirm`

배너 필드

로그인 시 사용자에게 표시될 배너 텍스트를 지정합니다. 최대 491자까지 가능합니다. 기본값은 없습니다. IPsec VPN 클라이언트는 배너에 대해 전체 HTML을 지원하지만, AnyConnect Client는 부분 HTML만 지원합니다. 원격 사용자에게 배너가 올바르게 표시되도록 하려면 IPsec 클라이언트에 /n 태그를 사용하고 SSL 클라이언트에는
 태그를 사용합니다.

DNS/WINS 필드

DNS(Domain Naming System) 및 WINS(Windows Internet Naming System) 서버입니다. AnyConnect Client 이름 전송에 사용합니다.

- 기본 **DNS** 서버 및 보조 **DNS** 서버 - 그룹에서 사용하려는 DNS 서버의 IPv4 또는 IPv6 주소를 정의하는 네트워크 개체를 선택 또는 생성합니다.
- 기본 **WINS** 서버 및 보조 **WINS** 서버 - 그룹에서 사용하려는 WINS 서버의 IP 주소를 포함하는 네트워크 개체를 선택 또는 생성합니다.
- **DHCP Network Scope(DHCP** 네트워크 범위**)** - 원하는 풀과 동일한 서브넷에서 풀에 포함되지 않는 라우팅 가능한 IPv4 주소를 포함하는 네트워크 개체를 선택하거나 생성합니다. DHCP 서버는 이 IP 주소가 속한 서브넷을 확인하고 해당 풀에서 IP 주소를 할당합니다. 설정이 올바르지 않은 경우 VPN 정책 구축이 실패합니다.

  연결 프로파일에서 주소 풀에 대한 DHCP 서버를 컨피그레이션하는 경우, DHCP 범위에서는 이 그룹에 대한 풀에 사용할 서브넷을 식별합니다. 또한 DHCP 서버 주소에는 해당 범위에서 식별하는 동일한 서브넷에 주소가 있어야 합니다. 이 범위를 통해 사용자는 DHCP 서버에 정의된 주소 풀의 하위 집합을 선택하여 이 특정 그룹에 사용할 수 있습니다.

  네트워크 범위를 정의하지 않으면 DHCP 서버에서 구성된 주소 풀 순으로 IP 주소를 할당합니다. 할당되지 않은 주소를 식별할 때까지 풀을 검색합니다.

  라우팅을 위해 가능한 경우 항상 인터페이스의 IP 주소를 사용하는 것이 좋습니다. 예를 들어 풀이 10.100.10.2-10.100.10.254이고 인터페이스 주소가 10.100.10.1/24이면 DHCP 범위로 10.100.10.1을 사용합니다. 네트워크 번호를 사용하지 마십시오. IPv4 주소 지정에만 DHCP를 사용할 수 있습니다. 선택한 주소가 인터페이스 주소가 아닌 경우 범위 주소에 대한 고정 경로를 생성해야 할 수 있습니다.

  LINK-SELECTION(RFC 3527) 및 SUBNET-SELECTION(RFC 3011)은 현재 지원되지 않습니다.
- 디폴트 도메인 - 기본 도메인의 이름입니다. 예를 들어 최상위 도메인으로 example.com을 지정합니다.

스플릿 터널링 필드

스플릿 터널링은 일부 네트워크 트래픽이 VPN 터널(암호화됨)을 통과하도록 유도하고 나머지 네트워크 트래픽은 VPN 터널 외부(암호화되지 않음 또는 "일반 텍스트 형식")로 보냅니다.

- **IPv4** 스플릿 터널링 **/ IPv6** 스플릿 터널링 - 기본적으로 스플릿 터널링은 활성화되어 있지 않습니다. IPv4 및 IPv6 모두 터널을 통해 모든 트래픽을 허용하도록 설정됩니다. 그대로 둘 경우 엔드포인트의 모든 트래픽은 VPN 연결을 통해 이동합니다.

스플릿 터널링을 구성하려면 아래에 지정된 터널 네트워크 또는 아래에 지정된 제외 네트워크 정책을 선택합니다. 그런 다음 해당 정책에 대해 액세스 제어 목록을 구성합니다.

- 스플릿 터널 네트워크 목록 유형 - 사용하는 액세스 목록의 유형을 선택합니다. 표준 액세스 목록 또는 확장 액세스 목록을 선택 또는 생성합니다. 자세한 내용은 액세스 목록, 20 페이지를 참조하십시오.
- **DNS** 요청 스플릿 터널링 - 스플릿 DNS라고도 합니다. 사용자 환경에서 예상 DNS 행동을 구성합니다.

  기본적으로 스플릿 DNS가 활성화되어 있지 않고 스플릿 터널 정책에 따라 **DNS** 요청 전송으로 설정됩니다. 항상 터널을 통해 **DNS** 요청 전송을 선택하면 모든 DNS 요청을 강제로 터널을 통해 프라이빗 네트워크에 전송합니다.

  스플릿 DNS를 구성하려면 지정된 도메인만 터널을 통해 전송을 선택하고 도메인 목록 필드에 도메인 이름 목록을 입력합니다. 이 요청은 스플릿 터널을 통해 프라이빗 네트워크로 전송됩니다. 다른 이름은 공용 DNS 서버를 통해 전송됩니다. 도메인 목록은 쉼표로 구분하여 최대 10개의 항목을 입력할 수 있습니다. 전체 문자열은 255자를 초과할 수 없습니다.

관련 항목

그룹 정책 개체 설정, 118 페이지

그룹 정책 **AnyConnect Client** 옵션

이러한 사양은 AnyConnect Client VPN의 작업에 적용됩니다.

탐색

Objects(개체**)** > **Object Management(**개체 관리**)** > **VPN** > **Group Policy(**그룹 정책**)**. **Add Group Policy(**그룹 정책 추가**)**를 클릭하거나 현재 정책을 선택하여 편집합니다. 그런 다음 **AnyConnect** 탭을 선택합니다.

프로파일 필드

프로파일 - AnyConnect Client 프로파일를 포함하는 파일 개체를 선택 또는 생성합니다. 개체 생성에 대한 자세한 내용은 파일 개체, 126 페이지을 참조하십시오.

AnyConnect Client 프로파일은 하나의 XML 파일에 설정 매개변수가 저장된 그룹입니다. AnyConnect Client 소프트웨어는 클라이언트의 사용자 인터페이스에 표시되는 연결 항목을 구성하는 데 사용합니다. 이러한 매개변수(XML 태그)는 더 많은 AnyConnect Client 기능을 활성화하는 설정을 구성합니다.

독립 설정 도구인 GUI 기반의 AnyConnect 프로파일 편집기을 사용하여 AnyConnect Client 프로파일를 생성합니다. 자세한 내용은 Cisco Secure Client(AnyConnect 포함) 관리자 가이드의 해당 릴리스에 있는 *AnyConnect* 프로파일 편집기 장을 참조하십시오.

관리 프로파일 필드

관리 VPN 터널은 엔드 유저가 VPN에 연결하지 않는 경우라도 엔트포인트가 켜져 있을 때마다 기업 네트워크에 대한 연결을 제공합니다.

관리 **VPN** 프로파일 - 관리 프로파일에는 엔드포인트에서 관리 VPN 터널을 자동으로 활성화하고 설정하기 위한 설정이 포함되어 있습니다.

독립형 관리 VPN 터널 프로파일 편집기를 사용하여 새 프로파일 파일을 생성하거나 기존 파일을 수정할 수 있습니다. Cisco 소프트웨어 다운로드 센터에서 프로파일 편집기를 다운로드할 수 있습니다.

프로파일 파일 추가에 대한 자세한 내용은 파일 개체, 126 페이지의 내용을 참조하십시오.

클라이언트 모듈 필드

Cisco AnyConnect VPN Only는 다양한 내장 모듈을 통해 향상된 보안을 제공합니다. 이러한 모듈은 웹 보안, 엔드 포인트 플로우에 대한 네트워크 가시성, 네트워크 외부 로밍 보호와 같은 서비스를 제공합니다. 각 클라이언트 모듈에는 요구 사항에 따라 사용자 지정 구성 그룹이 포함된 클라이언트 프로파일이 포함되어 있습니다.

다음 AnyConnect Client모듈은 선택 사항이며, VPN 사용자가 AnyConnect Client를 다운로드할 때 이러한 모듈을 다운로드하도록 설정할 수 있습니다.

- **AMP Enabler** — 엔드포인트용 AMP(Advanced Malware Protection)를 구축합니다.
- **DART** - 문제 해결을 위해 Cisco TAC로 전송할 수 있는 시스템 로그 및 기타 진단 정보의 스냅샷을 캡처합니다.
- **ISE Posture** — OPSWAT v3 라이브러리를 사용하여 엔드포인트의 컴플라이언스를 평가하기 위한 상태 확인을 수행합니다.
- **Network Access Manager** - 802.1X(계층 2)와 유선 및 무선 네트워크에 액세스하기 위한 디바이스 인증을 제공합니다.
- **Network Visibility(**네트워크 가시성**)** — 용량 및 서비스 계획, 감사, 컴플라이언스 및 보안 분석을 수행하기 위한 엔터프라이즈 관리자의 역량을 개선합니다.
- **Start Before Login(**로그인 전 시작**)**- Windows 로그인 대화 상자가 나타나기 전에 AnyConnectAnyConnect Client를 시작하여 Windows에 로그온하기 전에 VPN 연결을 통하여 사용자를 엔터프라이즈 인프라에 연결시킵니다.
- **Umbrella** 로밍 보안 — 활성 VPN이 없을 때 DNS 레이어 보안을 제공합니다.
- 웹 보안 - 정의된 보안 정책에 따라 웹 페이지의 요소를 분석하고 허용되는 콘텐츠를 허용하며 악성 또는 허용되지 않는 콘텐츠를 차단합니다.

Add(추가**)**를 클릭하고 각 클라이언트 모듈에 대해 다음을 선택합니다.

- 클라이언트 모듈 - 목록에서 AnyConnect Client 모듈을 선택합니다.
- 다운로드할 프로파일 - AnyConnect Client 프로파일를 포함하는 파일 개체를 선택 또는 생성합니다. 개체 생성에 대한 자세한 내용은 파일 개체, 126 페이지을 참조하십시오.
- **Enable module download(**모듈 다운로드 활성화**)** - 엔드포인트가 프로파일과 함께 클라이언트 모듈을 다운로드하도록 하려면 선택합니다. 선택하지 않으면 엔드포인트는 클라이언트 프로파일만 다운로드할 수 있습니다.

독립 구성 도구인 GUI 기반의 AnyConnect 프로파일 편집기을 사용하여 각 모듈에 대한 클라이언트 프로파일을 생성합니다. Cisco 소프트웨어 다운로드 센터에서 AnyConnect 프로파일 편집기를 다운로드합니다. 자세한 내용은 Cisco AnyConnect Secure Mobility Client 관리자 가이드의 해당 릴리스에 있는 *AnyConnect* 프로파일 편집기 장을 참조하십시오.

SSL 설정 필드

- **SSL** 압축 - 데이터 압축 활성화 여부를 선택하고, 활성화하는 경우 압축 해제 또는 LZS 중 사용할 데이터 압축 방법을 선택합니다. SSL 압축은 기본적으로 Disabled(비활성화) 상태입니다.

  데이터를 압축하면 전송 속도가 빨라지지만 각 사용자 세션에 대한 메모리 요건 및 CPU 사용량이 증가합니다. 그렇게 보안 어플라이언스의 전체 처리량이 감소합니다.

- **DTLS** 압축 - LZS를 사용해 그룹에 대한 DTLS(Datagram Transport Layer Security) 연결을 압축할지 여부를 선택합니다. DTLS 압축은 기본적으로 비활성화되어 있습니다.

- **MTU** 크기 — Cisco AnyConnect VPN Only에서 설정한 SSL VPN 연결의 MTU(Maximum Transmission Unit)입니다. 기본값은 1406바이트이며 유효범위는 576~1462바이트입니다.

  - **DF** 비트 무시 - 단편화가 필요한 패킷에서 DF(Don't Fragment) 비트를 무시할지 여부를 선택합니다. DF 비트가 설정된 패킷의 강제 조각화를 허용하여 터널을 통과할 수 있게 합니다.

연결 설정 필드

- **Anyconnect** 클라이언트와 **VPN** 게이트웨이 간 **Keepalive** 메시지 활성화, 간격 설정 - 피어 간 연결 유지 메시지를 교환하여 터널에서 데이터 송수신이 가능한지 시연 여부를 선택합니다. 기본적으로 활성화되어 있습니다. 연결 유지 메시지는 설정된 간격에 따라 전송됩니다. 활성화된 경우 IKE 연결 유지 패킷을 전송하고 원격 클라이언트가 대기하는 시간 간격(초 단위)을 입력합니다. 기본 간격은 20초, 유효 범위는 15~600초입니다.

- 데드 피어 탐지 활성화**...**. 간격 설정 - DPD(Dead Peer Detection)을 사용하면 VPN 보안 게이트웨이 또는 VPN 클라이언트는 피어가 응답하지 않으며 연결이 실패했음을 신속하게 감지합니다. 게이트웨이 및 클라이언트 모두에 기본적으로 활성화되어 있습니다. DPD 메시지는 설정된 간격에 따라 전송됩니다. 활성화된 경우 DPD 메시지를 전송하고 원격 클라이언트가 대기하는 시간 간격(초 단위)을 입력합니다. 기본 간격은 30초이며 유효 범위는 5~3600초입니다.

- 클라이언트 우회 프로토콜 활성화 - 이 옵션을 선택하면 보안 게이트웨이에서 (IPv6 트래픽만 예상할 때) IPv4 트래픽을 관리하는 방법 또는 (IPv4 트래픽만 예상할 때) IPv6 트래픽을 관리하는 방법을 구성할 수 있습니다.

  AnyConnect Client에서 헤드엔드와의 VPN 연결을 수행할 때 헤드엔드에서는 IPv4 주소나 IPv6 주소 또는 IPv4 및 IPv6 주소 모두를 지정합니다. 헤드엔드에서 AnyConnect Client 연결에 IPv4 주소만 또는 IPv6 주소만 지정할 경우, 헤드엔드에서 IP 주소를 지정하지 않은 네트워크 트래픽을 삭제하거나 이 트래픽이 헤드엔드를 우회하여 암호화되지 않은 또는 “일반 텍스트” 형태(활성화 및 확인된 상태)로 클라이언트에서 전송되는 것을 허용하도록 Client Bypass Protocol(클라이언트 우회 프로토콜)을 컨피그레이션할 수 있습니다.

  예를 들어 보안 게이트웨이에서 AnyConnect Client 연결에 IPv4 주소만 지정하고 엔드포인트는 이중 스택이라고 가정합시다. 엔드포인트가 IPv6 주소에 연결하려고 시도할 때 클라이언트 우회

프로토콜이 비활성화된 경우 IPv6 트래픽이 끊기지만 클라이언트 우회 프로토콜이 활성화된 경우, IPv6 트래픽은 클라이언트에서 암호화되지 않은 상태로 전송됩니다.

- **SSL** 키 재입력 - 클라이언트가 연결에 키를 재입력하여 암호화 키와 초기화 벡터를 재협상하고 연결 보안을 강화할 수 있습니다. 기본적으로 비활성화되어 있습니다. 활성화된 경우 지정된 간격으로 재협상이 발생하며 기존 터널에 키를 재입력하거나 다음 필드를 설정하여 새 터널을 생성합니다.
  - 방법 - SSL 키 재설정이 활성화되면 사용 가능합니다. 새 터널(기본값)을 생성하거나 기존 터널의 사양을 재협상합니다.
  - 간격 - SSL 키 재설정이 활성화되면 사용 가능합니다. 기본 범위는 4분이며 4-10080분(일주일) 범위 내에서 설정할 수 있습니다.
- 클라이언트 방화벽 규칙 - 클라이언트 방화벽 규칙을 사용하여 VPN 클라이언트 플랫폼에 대한 방화벽 설정을 구성합니다. 규칙은 소스 주소, 대상 주소 및 프로토콜 등의 기준을 기반으로 합니다. 확장 액세스 제어 목록 구성 요소 개체는 트래픽 필터 기준을 정의하는 데 사용됩니다. 이 그룹 정책에 대한 확장 ACL을 선택하거나 생성합니다. 프라이빗 네트워크의 데이터 플로우를 제어하는 프라이빗 네트워크 규칙과 설정된 VPN 터널 외부에 "있는 그대로" 데이터 플로우를 제어하는 공용 네트워크 규칙 또는 둘 다를 정의합니다.

참고 ACL이 TCP/UDP/ICMP/IP 포트를 포함하고 소스 네트워크가 any, any-ipv4 또는 any-ipv6을 포함하도록 확인합니다.

Microsoft Windows에서 실행되는 VPN 클라이언트만 이러한 방화벽 기능을 사용할 수 있습니다.

사용자 지정 속성 필드

이 섹션에는 앱별 VPN, 업그레이드 허용 또는 지연, 동적 스플릿 터널링과 같은 기능을 설정하기 위해 AnyConnect Client에서 사용하는 AnyConnect 사용자 지정 속성이 나와 있습니다. **Add(**추가**)**를 클릭하여 사용자 지정 속성을 그룹 정책에 추가합니다.

1. **AnyConnect Attribute(AnyConnect** 속성**)**(퍼 앱(Per App) VPN, 지연 업데이트 허용 또는 동적 스플릿 터널링)를 선택합니다.
2. 목록에서 **Custom Attribute Object(**사용자 지정 속성 개체**)**를 선택합니다.

참고 Add(+)(추가)를 클릭하여 선택한 AnyConnect 속성에 대한 새 사용자 지정 속성 개체를 생성합니다. **Objects(**개체**)** > **Object Management(**개체 관리**)** > **VPN** > **Custom Attribute(**사용자 지정 속성**)**에서 사용자 지정 속성 개체를 생성할 수도 있습니다. AnyConnect Client 사용자 지정 속성 개체 추가, 129 페이지의 내용을 참조하십시오.

3. **Add(**추가**)**를 클릭하여 속성을 그룹 정책에 저장한 다음 **Save(**저장**)**를 클릭하여 변경 사항을 그룹 정책에 저장합니다.

관련 항목

그룹 정책 개체 설정, 118 페이지

그룹 정책 고급 옵션

탐색 경로

Objects(개체**)** > **Object Management(**개체 관리**)** > **VPN** > **Group Policy(**그룹 정책**)**의 경우 **Add Group Policy(**그룹 정책 추가**)**를 클릭하거나 현재 정책을 선택하여 편집합니다.을 클릭하고 고급 탭을 선택합니다.

트래픽 필터

- 액세스 목록 필터 - VPN 연결을 통해 수신되는 터널링된 데이터 패킷을 허용 또는 차단할지 여부를 결정하는 규칙으로 구성된 필터입니다. 규칙은 소스 주소, 대상 주소 및 프로토콜 등의 기준을 기반으로 합니다. VPN 필터는 초기 연결에만 적용됩니다. 애플리케이션 검사 작업으로 인해 열리는 SIP 미디어 연결과 같은 보조 연결에는 적용되지 않습니다. 확장 액세스 제어 목록 구성 요소 개체는 트래픽 필터 기준을 정의하는 데 사용됩니다. 이 그룹 정책에 대한 새 확장 ACL을 선택하거나 생성합니다.
- **VPN**을 **VLAN**으로 제한 - "VLAN 매핑"이라고도 하는 이 파라미터는 이 그룹 정책이 적용되는 세션에 이그레스 VLAN 인터페이스를 지정합니다. ASA에서는 이 그룹의 모든 트래픽을 선택된 VLAN으로 전달합니다.

  이 특성을 사용하여 그룹 정책에 VLAN을 할당하면 액세스 제어를 간소화할 수 있습니다. ACL을 사용하여 세션의 트래픽을 필터링하는 방법 대신 이 특성에 값을 할당하는 방법도 가능합니다. 기본값(Unrestricted(제한 없음)) 이외에는 이 ASA에 구성된 VLAN만 드롭다운 목록에 표시됩니다. 허용된 값의 범위는 1에서 4094까지입니다.

세션 설정 필드

- 액세스 시간 - 시간 범위 개체를 선택 또는 생성합니다. 이 개체는 이 그룹 정책이 원격 액세스 사용자에게 적용할 수 있는 시간 범위를 지정합니다. 자세한 내용은 시간 범위, 91 페이지를 참조하십시오.
- 사용자당 동시 로그인 수 - 사용자에게 허용되는 최대 동시 로그인 수를 지정합니다. 기본값은 3입니다. 최소값은 0이며, 이 경우 로그인이 비활성화되고 사용자 액세스가 차단됩니다. 다수의 동시 연결을 허용하면 보안이 취약해지고 성능이 저하될 수 있습니다.
- 최대 연결 시간 / 알림 간격 - 최대 사용자 연결 시간을 분 단위로 설정합니다. 이 시간이 경과하면 시스템은 자동으로 연결을 종료합니다. 최소값은 1분입니다). 알림 간격은 최대 연결 시간에 도달하기 전 사용자에게 메시지를 표시하는 시간 간격입니다.
- 유휴 시간 제한 / 알림 간격 - 사용자의 유휴 시간 제한 기간을 분 단위로 지정합니다. 이 기간 동안 사용자 연결을 통한 통신 활동이 없는 경우 시스템은 연결을 종료합니다. 최소값은 1분입니다. 기본값은 30분입니다. 알림 간격은 유휴 시간 제한에 도달하기 전 사용자에게 메시지를 표시하는 시간 간격입니다.

관련 항목

그룹 정책 개체 설정, 118 페이지

파일 개체

파일 개체를 생성 및 편집하려면 파일 개체 추가 및 편집 대화 상자를 사용합니다. 파일 개체는 컨피그레이션(일반적으로 원격 액세스 VPN 정책)에서 사용되는 파일을 나타냅니다. AnyConnect Client 프로파일, AnyConnect Client 이미지 파일을 포함할 수 있습니다.

프로파일은 또한 독립 프로파일 편집기를 사용하여 각 AnyConnect 모듈 및 AnyConnect Client Management VPN에 대해 생성되고 AnyConnect의 일부로 엔드포인트에서 관리자 정의 최종 사용자 요건 및 인증 정책에 구축되어 있으며 미리 설정된 네트워크 프로파일을 최종 사용자가 사용할 수 있게 설정되어 있습니다.

파일 개체를 생성하는 경우 management center은 저장소에서 파일의 복사본을 만듭니다. 이러한 파일은 데이터베이스 백업을 생성할 때마다 백업되고 데이터베이스를 복원하는 경우 복원됩니다. 파일 개체에 사용하기 위해 파일을 플랫폼에 복사하는 경우, 파일 저장소를 파일 디렉토리에 복사하지 마십시오.

특정 파일 개체를 지정하는 설정을 구축하는 경우 관련 파일은 디바이스의 적절한 디렉터리에 다운로드됩니다.

각 파일에 대해 다음 옵션 중 하나를 클릭할 수 있습니다.

- **Download(**다운로드**)** - AnyConnect 파일을 다운로드하려면 클릭합니다.
- **Edit(**수정**)** - 파일 개체 세부 사항을 수정합니다.
- **Delete(**삭제**)** - AnyConnect Client 파일 개체를 삭제합니다. 파일 개체를 삭제하면 파일 저장소에서 관련 파일은 삭제되지 않고 개체만 삭제됩니다.

탐색 경로

Objects(개체**)** > **Object Management(**개체 관리**)** > **VPN** > **AnyConnect File(AnyConnect** 파일**)**.

필드

- **Name(**이름**)** - 파일 개체를 식별할 파일의 이름을 입력합니다. 최대 128자를 추가할 수 있습니다.
- **File Name(**파일 이름**)**—**Browse(**찾아보기**)**를 클릭하여 이미지 파일을 선택합니다. 파일을 선택하면 파일 이름과 파일의 전체 경로가 추가됩니다.
- **File Type(**파일 유형**)** - 선택한 파일에 해당하는 파일 유형을 선택합니다. 다음 파일 유형을 사용할 수 있습니다.
  - **AnyConnect Client Image** - Cisco 소프트웨어 다운로드 센터에서 다운로드한 AnyConnect Client 클라이언트 이미지를 추가할 때 이 유형을 선택합니다.

    사용자는 새 AnyConnect Client 이미지 또는 추가 이미지를 VPN 정책에 연결할 수 있습니다. 또한 지원되지 않거나 단종되었으며 더 이상 필요하지 않은 클라이언트 패키지의 연결을 해제할 수 있습니다.

- **AnyConnect VPN** 프로파일—AnyConnect VPN 프로파일 파일에 대해 이 유형을 선택합니다.

  프로파일 파일은 독립적인 설정 도구인 GUI 기반의 AnyConnect 프로파일 편집기를 사용하여 생성됩니다. 자세한 내용은 Cisco AnyConnect Secure Mobility Client 관리자 가이드 의 해당 릴리스에 있는 *AnyConnect* 프로파일 편집기 장을 참조하십시오.

- **AnyConnect Management VPN** 프로파일 - AnyConnect 관리 VPN 터널에 대한 프로파일 파일을 추가할 때 이 유형을 선택합니다.

  Cisco 소프트웨어 다운로드 센터에서 AnyConnect **VPN** 관리 터널 독립형 프로파일 편집기를 다운로드하지 않은 경우 다운로드하고 AnyConnect 관리 VPN 터널에 필요한 설정으로 프로파일을 생성합니다.

- **AMP Enabler** 서비스 프로파일 - 이 프로파일은 AnyConnect AMP Enabler에 사용됩니다. 원격 액세스 VPN 사용자가 VPN에 연결하면 이 프로파일과 함께 AMP Enabler가 threat defense에서 엔드 포인트로 푸시됩니다.

- 피드백 프로파일 - 고객 경험 피드백 프로파일을 추가하고 이 유형을 선택하여 고객이 활성화하고 사용하는 기능 및 모듈에 대한 정보를 수신할 수 있습니다.

- **ISE Posture** 프로파일 - AnyConnect ISE Posture 모듈용 프로파일 파일을 추가하는 경우 이 옵션을 선택합니다.

- **NAM** 서비스 프로파일 - Network Access Manager 프로파일 편집기를 사용하여 NAM 프로파일 파일을 설정하고 추가합니다.

- 네트워크 가시성 서비스 프로파일 - AnyConnect 네트워크 가시성 모듈의 프로파일 파일입니다. NVM 프로파일 편집기를 사용하여 프로파일을 생성할 수 있습니다.

- **Umbrella** 로밍 보안 프로파일 - 프로파일 편집기를 사용하여 생성한 .json 파일을 사용하여 Umbrella 로밍 보안 모듈을 구축하는 경우 이 파일 유형을 선택해야 합니다.

- 웹 보안 서비스 프로파일 - 웹 보안 모듈용 프로파일 파일을 추가할 때 이 파일 유형을 선택합니다.

- **HostScan** 패키지 - HostScan 패키지 파일을 추가할 때 이 파일 유형을 선택합니다. 이 파일은 엔드포인트에 설치된 운영 체제, 안티바이러스, 안티스파이웨어 및 방화벽 소프트웨어에 대한 정보를 수집하기 위해 DAP(Dynamic Access Policy)를 구성하는 동안 사용됩니다.

- **AnyConnect** 외부 브라우저 패키지 - 이 파일 유형은 SAML SSO(Single Sing-On) 인증을 위한 외부 브라우저 패키지 파일을 선택하는 데 사용됩니다.

  외부 패키지 파일의 새 버전을 사용할 수 있는 경우 패키지 파일을 추가할 수 있습니다.

  자세한 내용은 Remote Access VPN에 대한 AAA 설정를 참고하십시오.

- 설명 - 필요한 설명을 추가합니다.

관련 항목

Cisco AnyConnect Security Mobility Client 이미지

그룹 정책 AnyConnect Client 옵션, 121 페이지

인증서 맵 개체

인증서 맵 개체는 명명된 인증서 일치 규칙 집합입니다. 이런 개체는 수신된 인증서 및 원격 액세스 VPN 연결 프로파일 간 연결을 제공하는 데 사용됩니다. 연결 프로파일 및 인증서 맵 개체는 원격 액세스 VPN 정책의 일부입니다. 수신된 인증서가 인증서 맵에 포함된 규칙과 일치하는 경우 해당 연결은 "매핑되거나" 지정된 연결 프로파일에 연결됩니다. 규칙은 우선 순위에 따라 UI에 표시된 순서대로 적용됩니다. 인증서 맵 개체 내에서 첫 번째 규칙이 일치하는 경우 일치가 종료됩니다.

탐색

개체 > 개체 관리 > **VPN** > 인증서 맵

필드

- 이름 - 개체를 식별하여 원격 액세스 VPN 등 다른 설정에서 참조할 수 있도록 합니다.
- 매핑 기준-평가하기 위한 인증서의 내용을 지정합니다. 인증서가 이런 규칙을 만족시키는 경우 사용자는 이 개체를 포함하는 연결 프로파일에 매핑됩니다.
  - 구성 요소-일치시키는 규칙에 사용될 클라이언트 인증서의 구성 요소를 선택합니다.
  - 필드-클라이언트 인증서의 발급자 또는 제목에 따라 일치시키는 규칙에 대한 필드를 선택합니다.

    필드가 대체 제목 또는 확장 키 사용인 경우 구성 요소는 전체 필드여야 합니다.
  - 연산자-다음과 같은 일치 조건에 대한 연산자를 선택합니다.
    - 같음 - 인증서 구성 요소가 입력한 값과 일치해야 합니다. 정확하게 일치하지 않으면 연결이 거부됩니다.
    - 포함 - 인증서 구성 요소가 입력한 값을 포함해야 합니다. 구성 요소에 해당 값이 포함되지 않으면 연결이 거부됩니다.
    - 같지 않음 - 인증서 구성 요소가 입력한 값과 일치하면 안 됩니다. 예를 들어 인증서 요소 중 국가를 선택하고 입력한 값이 US인 경우, 클라이언트 국가 값이 US와 같다면 해당 연결이 거부됩니다.
    - 포함되어 있지 않음 - 인증서 구성 요소가 입력한 값을 포함하면 안 됩니다. 예를 들어 인증서 요소 중 국가를 선택하고 입력한 값이 US인 경우, 클라이언트 국가 값에 US를 포함하면 해당 연결이 거부됩니다.
- 값-일치 규칙의 값입니다. 입력한 값은 선택된 구성 요소 및 연산자와 연결됩니다.

관련 항목

인증서 맵 구성

AnyConnect Client 사용자 지정 속성 개체

맞춤 속성은 앱별 VPN, 업그레이드 허용 또는 지연, 동적 스플릿 터널링과 같은 기능을 구성하기 위해 AnyConnect Client에서 사용됩니다. 사용자 지정 특성에는 유형 및 명명된 값이 있습니다. 먼저 특성의 유형을 정의한 다음 이 유형의 명명된 값을 하나 이상 정의할 수 있습니다. management center를 사용하여 AnyConnect 맞춤 속성 개체를 생성하고, 개체를 그룹 정책에 추가하고, 그룹 정책을 원격 액세스 VPN과 연결하여 VPN 클라이언트에 대한 기능을 활성화할 수 있습니다.

Threat Defense는 맞춤 속성 개체를 사용하여 다음 기능을 지원합니다.

- **Per App VPN** - Per App VPN 기능은 threat defense 관리자가 VPN을 통해 허용하는 앱 및 터널 전용 애플리케이션을 식별하는 데 도움이 됩니다.
- **Allow or defer upgrade(**업그레이드 허용 또는 보류**)**—Deferred Upgrade(보류 업그레이드)를 통해 AnyConnect Client 사용자는 AnyConnect Client 업그레이드 다운로드를 지연시킬 수 있습니다. 클라이언트 업데이트를 사용할 수 있는 경우 AnyConnect Client 속성을 구성해서 사용자에게 업데이트할지 또는 업그레이드를 보류할지 묻는 대화 상자가 열리도록 할 수 있습니다.
- 동적 스플릿 터널링 - 동적 스플릿 터널링을 사용하면 VPN 터널에서 IP 주소 또는 네트워크를 포함하거나 제외하는 정책을 프로비저닝할 수 있습니다. 맞춤형 속성을 생성한 다음 그룹 정책에 추가하는 방식으로 동적 스플릿 터널링을 구성합니다.

AnyConnect Client 맞춤 속성을 구성하기 위한 단계별 지침은 AnyConnect Client 사용자 지정 속성 개체 추가, 129 페이지의 내용을 참조하십시오.

특정 기능에 대해 구성할 특정 맞춤 속성에 대한 자세한 내용은 사용 중인 사용 중인 AnyConnect Client 릴리스에 대한 *Cisco Secure Client(AnyConnect* 포함*)* 관리자 가이드를 참조하십시오.

관련 항목

그룹 정책 AnyConnect Client 옵션, 121 페이지

AnyConnect Client 사용자 지정 속성 개체 추가

시작하기 전에

앱별 VPN에 대한 맞춤형 속성 개체를 추가하기 전에 다음을 수행했는지 확인하십시오.

- 앱별 VPN은 MDM을 통해 올바르게 설정해야 하며 각 디바이스는 MDM 서버에 등록되어야 합니다.
- Cisco AnyConnect Client 엔터프라이즈 애플리케이션 선택기 툴을 사용하여 각 앱에 대해 base64 인코딩 문자열을 생성합니다.
  1. 여기에서 Cisco AnyConnect Client 엔터프라이즈 애플리케이션 선택기 툴을 다운로드합니다.
  2. 애플리케이션 선택 툴을 열고 왼쪽 상단에 있는 드롭다운 메뉴에서 모바일 플랫폼을 선택합니다.
  3. 식별 이름 및 앱 ID를 입력하여 규칙을 추가합니다. 나머지 필드는 선택 사항입니다.
  4. 메뉴 모음에서 정책을 클릭합니다. 인코딩된 base65 규칙은 인코딩된 형식으로 표시됩니다.

5. 정책 문자열을 선택하여 복사한 다음, 나중에 AnyConnect Client 맞춤형 속성 개체를 생성할 때 사용할 수 있도록 저장합니다.

프로시저

단계 **1** **Objects(**개체**)** > **Object Management(**개체 관리**)** > **VPN** > **Custom Attributes(**맞춤형 속성**)**를 선택합니다.

단계 **2** **AnyConnect Custom Attributes(**사용자 지정 속성**)**을 클릭합니다.

단계 **3** 속성의 **Name(**이름**)**을 입력하고 필요한 경우, **Description(**설명**)**을 입력합니다.

단계 **4** **AnyConnect Attribute(AnyConnect** 속성**)** 드롭다운 목록에서 속성을 선택합니다.

- **Per App VPN(**앱별 **VPN)** - 이 옵션을 선택하고 **Attribute Value(**속성 값**)** 상자에 base64 인코딩 문자열을 지정합니다.
- **Allow Defer Update (**업데이트 연기 허용**)** - 다음 옵션 중 하나를 선택하고 AnyConnect Client 업데이트 연기를 허용하는 데 필요한 정보를 지정합니다.
  - **Show the prompt until user takes action(**사용자가 작업을 수행할 때까지 프롬프트 표시**)** - 사용자가 VPN 클라이언트 업데이트를 허용하거나 연기하도록 선택할 때까지 VPN 사용자에게 프롬프트를 표시합니다.
  - **Show the prompt until times out(**시간 초과될 때까지 프롬프트 표시**)** - 지정된 기간 동안 프롬프트를 표시하고 **Timeout(**시간 초과**)** 상자에서 기간을 지정하려면 이 옵션을 선택합니다.
  - **Do not show the prompt and take automatic action(**프롬프트를 표시하지 않고 자동 작업 수행**)** - VPN 업데이트를 자동으로 허용하거나 연기하려면 이 옵션을 선택합니다.
  - **Default Action(**기본 작업**)** - 사용자가 응답하지 않거나 사용자의 개입 없이 자동 작업을 설정하려는 경우 수행할 기본 작업을 선택합니다. AnyConnect Client를 업데이트하거나 업데이트를 연기하도록 선택할 수 있습니다.
  - **Minimum Version(**최소 버전**)** - 업데이트를 허용하거나 연기하기 위해 클라이언트 시스템에 표시할 최소 AnyConnect 버전을 지정합니다.
- **Dynamic Split Tunneling(**동적 스플릿 터널링**)** - VPN 터널에서 IP 주소 또는 네트워크를 포함하거나 제외하려면 이 옵션을 선택합니다.
  - **Include domains(**도메인 포함**)** - 원격 접속 VPN 터널에 포함할 도메인 이름을 지정합니다.
  - **Exclude domains(**도메인 제외**)** - 원격 접속 VPN 터널에서 제외할 도메인 이름을 지정합니다.

단계 **5** 개체 오버라이드를 허용하려면 **Allow Overrides(**오버라이드 허용**)** 체크 박스를 선택합니다.

단계 **6** **Save(**저장**)**를 클릭합니다.
사용자 지정 속성 개체가 목록에 추가됩니다.

다음에 수행할 작업

사용자 지정 속성을 그룹 정책과 연결합니다. 그룹 정책에 사용자 지정 속성 추가, 131 페이지의 내용을 참조하십시오.

그룹 정책에 사용자 지정 속성 추가

AnyConnect 사용자 지정 속성을 원격 액세스 VPN 연결에 사용하려면 그룹 정책과 연결해야 합니다. 사용자

프로시저

단계 **1** **Objects(**개체**)** > **Object Management(**개체 관리**)** > **VPN** > **Group Policy(**그룹 정책**)**을 선택합니다.

단계 **2** 새 그룹 정책을 추가하거나 기존 그룹 정책을 편집합니다.

단계 **3** **AnyConnect** > **Custom Attributes(**사용자 지정 속성**)**을 클릭합니다.

단계 **4** **Add(**추가**)**를 클릭합니다.

단계 **5** **AnyConnect Attribute(AnyConnect** 속성**)**(퍼 앱(Per App) VPN, 지연 업데이트 허용 또는 동적 스플릿 터널링)를 선택합니다.

단계 **6** 목록에서 **Custom Attribute Object(**사용자 지정 속성 개체**)**를 선택합니다.

참고 Add(+)(추가)를 클릭하여 선택한 AnyConnect 속성에 대한 새 사용자 지정 속성 개체를 생성합니다. **Objects(**개체**)** > **Object Management(**개체 관리**)** > **VPN** > **Custom Attribute(**사용자 지정 속성**)**에서 사용자 지정 속성 개체를 생성할 수도 있습니다. AnyConnect Client 사용자 지정 속성 개체 추가, 129 페이지의 내용을 참조하십시오.

단계 **7** **Add(**추가**)**를 클릭하여 속성을 그룹 정책에 저장한 다음 **Save(**저장**)**를 클릭하여 변경 사항을 그룹 정책에 저장합니다.

관련 항목

그룹 정책 AnyConnect Client 옵션, 121 페이지

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.