도메인 관리

다음 주제는 도메인을 사용해 멀티 테넌시를 관리하는 방법을 설명합니다.

도메인을 사용하는 다중 테넌시 소개

Firepower System을 사용 하면 도메인을 사용 하는 멀티 테 넌 시를 구현할 수 있습니다. 도메인에 따라 매니지드 디바이스, 구성 및 이벤트에 대한 사용자 액세스가 구분됩니다. 최고 수준 글로벌 도메인에 2~3개의 레벨로 최대 100개의 하위 도메인을 생성할 수 있습니다.

Firepower Management Center에 로그인하는 경우, *current domain(*현재 도메인*)*이라고 하는 단일 도메인에 로그인합니다. 사용자 어카운트에 따라 다른 도메인으로 전환할 수 있습니다.

사용자 역할에 의해 부과된 제한 외에도 현재 도메인 레벨이 다양한 Firepower System 구성을 수정할 수 있는 기능을 제한할 수 있습니다. 시스템은 시스템 소프트웨어 업데이트와 같은 대부분의 관리 작업을 전역 도메인으로 제한합니다.

시스템은 다른 작업을 하위 도메인이 없는 리프 도메인으로 제한합니다. 예를 들어 각 매니지드 디비아스를 리프 도메인과 연결하고 해당 리프 도메인의 컨텍스트에서 디바이스 관리 작업을 수행해야 합니다.

각 리프 도메인은 해당 리프 도메인의 디바이스에서 수집한 검색 데이터를 기반으로 자체 네트워크 맵을 작성합니다. 매니지드 디바이스에서 보고한 이벤트(연결, 침입, 악성코드 등)도 디바이스의 리프 도메인에 연결됩니다.

도메인 레벨 **1:** 전역

멀티 테넌시를 구성하지 않는 경우, 모든 디바이스, 설정 및 이벤트가 전역 도메인에 속하며 이 시나리오에서는 리프 도메인이기도 합니다. 도메인 관리를 제외하고 시스템은 하위 도메인이 추가될 때까지 도메인별 구성 및 분석 옵션을 숨깁니다.

두 개의 도메인 레벨**:** 전역 및 **2**차 레벨

2단계 다중 도메인 구축에서 전역 도메인에는 직계 하위 도메인만 있습니다. 예를 들어 MSSP(매니지드 보안 서비스 제공자)는 여러 고객에 대한 네트워크 보안을 관리하기 위해 단일 Firepower Management Center를 사용할 수 있습니다.

- 전역 도메인에 로그인하는 MSSP 관리자는 고객의 구축을 보거나 편집할 수 없습니다. 고객의 구축을 관리하려면 각각 두 번째 수준의 명명된 하위 도메인에 로그인해야 합니다.
- 각 고객의 관리자는 두 번째 수준의 이름이 지정된 하위 도메인에 로그인하여 조직에 적용 가능한 디바이스, 구성 및 이벤트만 관리할 수 있습니다. 이런 로컬 관리자는 MSSP 내 다른 고객의 구축을 보거나 영향을 줄 수 없습니다.

세 개의 도메인 레벨**:** 전역**, 2**차 레벨 및 **3**차 레벨

3단계 다중 도메인 구축에서 전역 도메인에는 하위 도메인이 있으며, 그 중 적어도 하나가 자체 하위 도메인입니다. 앞의 예를 확장해, 이미 하위 도메인으로 제한되어 있는 MSSP 고객이 구축을 더욱 세분화하려는 시나리오를 생각해 보겠습니다. 이 고객은 디바이스 두 부류를 따로 관리하고자 합니다(네트워크 에지에 배치된 디바이스 및 내부에 배치된 디바이스).

- 두 번째 수준 하위 도메인에 로그인하는 고객의 관리자는 고객의 엣지 네트워크 구축을 보거나 편집할 수 없습니다. 네트워크 엣지에 구축된 디바이스를 관리하려면 해당 리프 도메인에 로그인해야 합니다.
- 고객의 엣지 네트워크 관리자는 세 번째 수준(리프) 도메인에 로그인하여 네트워크 엣지에 구축된 디바이스에 적용 가능한 디바이스, 구성 및 이벤트만 관리할 수 있습니다. 마찬가지로 고객의 내부 네트워크 관리자는 내부 디바이스, 구성 및 이벤트를 관리하기 위해 다른 3차 도메인에 로그인할 수 있습니다. 엣지 및 내부 관리자는 서로의 구축을 볼 수 없습니다.

참고 멀티테넌시를 사용하는 FMC에서 SSO 설정은 전역 도메인 수준에서만 적용할 수 있으며, 전역 도메인과 모든 하위 도메인에 적용됩니다.

관련 항목

SAML SSO(Single Sign-On) 구성

도메인 용어

이 문서에서는 도메인 및 다중 도메인 배포에 대해 다음 용어를 사용합니다.

전역 도메인

다중 도메인 구축의 경우, 최상위 도메인을 표시 합니다. 멀티 테넌시를 구성하지 않는 경우 모든 디바이스, 설정 및 이벤트는 전역 도메인에 해당됩니다. 관리자가 전역 도메인의 전체 Firepower System 구축을 관리할 수 있습니다.

서브도메인

이차 또는 삼차 도메인입니다.

이차 도메인

전역 도메인의 하위 도메인입니다. 이차 도메인은 리프 도메인 또는 하위 도메인이 될 수 있습니다.

삼차 도메인

이차 도메인의 하위 도메인입니다. 삼차 도메인은 항상 리프 도메인입니다.

리프 도메인

하위 도메인이 없는 도메인입니다. 각 디바이스는 리프 도메인에 속해야 합니다.

하위 도메인

계층 구조에서 현재 도메인의 하위 단계에 있는 도메인입니다.

하위 도메인

도메인의 직접 하위 도메인입니다.

최상위 도메인

현재 도메인을 하위 도메인으로 갖는 도메인입니다.

상위 도메인

도메인의 직접 상위 도메인입니다.

동기 도메인

상위 도메인이 동일한 도메인입니다.

현재 도메인

현재 로그인한 도메인입니다. 시스템은 웹 인터페이스의 오른쪽 상단 사용자 이름 앞에 현재 도메인의 이름을 표시합니다. 사용자 역할이 제한된 경우가 아니라면 현재 도메인의 설정을 수정할 수 있습니다.

도메인 속성

도메인 속성을 수정하려면 해당 도메인의 상위 도메인에서 관리자 권한이 있어야 합니다.

이름 및 설명

각 도메인의 이름은 계층 내에서 고유해야 합니다. 설명은 선택 사항입니다.

상위 도메인

두 번째 및 세 번째 레벨 도메인에는 상위 도메인이 있습니다. 도메인을 생성한 후에는 도메인의 상위 항목을 변경할 수 없습니다.

디바이스

리프 도메인만 디바이스를 포함할 수 있습니다. 즉, 도메인은 하위 도메인이나 디바이스 중 하나만 포함할 수 있으며 둘 다 포함할 수는 없습니다. 리프가 아닌 도메인이 디바이스를 직접 제어하는 구축은 저장할 수 없습니다.

도메인 편집기에서 웹 인터페이스에는 도메인 계층 내의 현재 위치에 따라 사용 가능한 디바이스와 선택한 디바이스가 표시됩니다.

호스트 제한

Firepower Management Center에서 모니터링할 수 있는 호스트, 즉 네트워크 맵에 저장할 수 있는 호스트 수는 해당 모델에 따라 다릅니다. 다중 도메인 구축에서 리프 도메인은 모니터링되는 호스트의 사용 가능 풀을 공유하지만, 네트워크 맵은 각기 다릅니다.

각 리프 도메인이 네트워크 맵을 채울 수 있도록 각 하위 도메인 레벨에서 호스트 제한을 설정할 수 있습니다. 도메인의 호스트 제한을 **0**으로 설정하면 도메인이 일반 풀을 공유합니다.

호스트 제한을 설정할 때 각 도메인 레벨에 미치는 영향은 서로 다릅니다.

- 리프 - 리프 도메인의 경우 호스트 제한은 리프 도메인이 모니터링할 수 있는 호스트 수에 대한 단순한 제한입니다.
- 두 번째 레벨 - 세 번째 레벨 리프 도메인을 관리하는 두 번째 레벨 도메인의 경우 호스트 제한은 리프 도메인이 모니터링할 수 있는 총 호스트 수를 나타냅니다. 리프 도메인은 사용 가능한 호스트 풀을 공유합니다.
- 글로벌 - 글로벌 도메인의 경우 호스트 제한은 Firepower Management Center에서 모니터링할 수 있는 총 호스트 수와 같습니다. 이 값은 변경할 수 없습니다.

하위 도메인의 호스트 제한을 합한 값이 상위 도메인의 호스트 제한보다 커질 수 있습니다. 예를 들어 글로벌 도메인 호스트 제한이 150,000이면 각기 호스트 제한이 100,000인 하위 도메인을 여러 개 구성할 수 있습니다. 이러한 각 도메인은 100,000개의 호스트를 모니터링할 수 있지만 모든 도메인이 100,000개의 호스트를 모니터링할 수 있는 것은 아닙니다.

네트워크 검색 정책은 호스트 제한에 도달한 후 새 호스트가 탐지될 때 수행되는 작업을 제어합니다. 새 호스트를 삭제하거나 가장 오랫동안 비활성 상태였던 호스트를 교체할 수 있습니다. 각 리프 도메인에 자체 네트워크 검색 정책이 있으므로, 각 리프 도메인은 시스템에서 새 호스트를 검색할 때 고유한 동작을 관리합니다.

도메인의 호스트 제한을 줄이는 경우 네트워크 맵에 새 제한보다 많은 호스트가 포함되어 있으면 가장 오랫동안 비활성 상태였던 호스트가 삭제됩니다.

관련 항목

Firepower System 호스트 제한
네트워크 검색 데이터 스토리지 설정

도메인 요구 사항 및 사전 요건

모델 지원

모두

지원되는 도메인

모든

사용자 역할

- 관리자

도메인 관리

도메인 속성을 수정하려면 해당 도메인의 상위 도메인에서 관리자 권한이 있어야 합니다.

프로시저

단계 **1** **System(**시스템**)** > **Domains(**도메인**)**를 선택합니다.

단계 **2** 도메인을 관리합니다.

- Add(추가) - **Add Domain(**도메인 추가**)**을 클릭하거나 상위 도메인 옆에 있는 **Add Subdomain(**하위 도메인 추가**)**을 클릭합니다. 새 도메인 생성, 6 페이지를 참조하십시오.
- Edit(수정) - 수정할 도메인 옆에 있는 아이콘(수정( ))을 클릭합니다. 도메인 속성, 3 페이지를 참조하십시오.
- Delete(삭제) - 삭제할 빈 도메인 옆에 있는 아이콘(삭제( ))을 클릭한 다음 선택 내용을 확인합니다. 대상 도메인을 수정하여 삭제할 도메인에서 디바이스를 이동합니다.

단계 **3** 도메인 구조를 변경하고 모든 디바이스를 리프 도메인과 연결한 후에 **Save(**저장**)**를 클릭하여 변경사항을 구현합니다.

단계 **4** 메시지가 표시되면 추가로 다음과 같이 변경합니다.

- 리프 도메인을 상위 도메인으로 변경한 경우 이전 네트워크 맵을 이동하거나 삭제합니다. 도메인 간 데이터 이동, 7 페이지를 참조하십시오.
- 도메인 간에 디바이스를 이동했으며 새 정책과 보안 영역 을 할당해야 하는 경우 도메인 간 디바이스 이동, 7 페이지를 참조하십시오.

다음에 수행할 작업

- 모든 새 도메인에 대한 사용자 역할 및 정책(액세스 제어, 네트워크 검색 등)을 구성합니다. 필요한 경우 디바이스 속성을 업데이트합니다.
- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축의 내용을 참조하십시오.

새 도메인 생성

최고 수준 글로벌 도메인에 2~3개의 레벨로 최대 100개의 하위 도메인을 생성할 수 있습니다.

모든 디바이스를 리프 도메인에 할당해야 도메인 컨피그레이션을 구현할 수 있습니다. 리프 도메인에 하위 도메인을 추가하면 도메인은 더 이상 리프 도메인이 아니며, 해당 도메인의 디바이스를 재할당해야 합니다.

프로시저

단계 **1** 글로벌 또는 두 번째 수준 도메인에서 **System(**시스템**)** > **Domains(**도메인**)**를 선택합니다.

단계 **2** **Add Domain(**도메인 추가**)**을 클릭하거나 상위 도메인 옆에 있는 **Add Subdomain(**하위 도메인 추가**)**을 클릭합니다.

단계 **3** **Name(**이름**)** 및 **Description(**설명**)**을 입력합니다.

단계 **4** **Parent Domain(**상위 도메인**)**을 선택합니다.

단계 **5** **Devices(**디바이스**)**에서 도메인에 추가할 **Available Devices(**사용 가능한 디바이스**)**를 선택한 다음 **Add to Domain(**도메인에 추가**)**을 클릭하거나 **Selected Devices(**선택한 디바이스**)** 목록으로 끌어다 놓습니다.

단계 **6** 필요한 경우 **Advanced(**고급**)**을 클릭하여 새 도메인이 모니터링할 수 있는 호스트 수를 제한합니다. 도메인 속성, 3 페이지를 참조하십시오.

단계 **7** **Save(**저장**)**를 클릭하여 도메인 관리 페이지로 돌아갑니다.

리프 도메인이 아닌 도메인에 할당된 디바이스가 있는지 확인하라는 경고가 표시됩니다. **Create New Domain(**새 도메인 생성**)**을 클릭하여 해당 디바이스용으로 새 도메인을 생성합니다. 디바이스를 기존 도메인으로 이동하려는 경우에는 **Keep Unassigned(**미할당 상태 유지**)**를 클릭합니다.

단계 **8** 도메인 구조를 변경하고 모든 디바이스를 리프 도메인과 연결한 후에 **Save(**저장**)**를 클릭하여 변경사항을 구현합니다.

단계 **9** 메시지가 표시되면 추가로 다음과 같이 변경합니다.

- 리프 도메인을 상위 도메인으로 변경한 경우 이전 네트워크 맵을 이동하거나 삭제합니다. 도메인 간 데이터 이동, 7 페이지를 참조하십시오.
- 도메인 간에 디바이스를 이동했으며 새 정책과 보안 영역 을 할당해야 하는 경우 도메인 간 디바이스 이동, 7 페이지를 참조하십시오.

다음에 수행할 작업

- 모든 새 도메인에 대한 사용자 역할 및 정책(액세스 제어, 네트워크 검색 등)을 구성합니다. 필요한 경우 디바이스 속성을 업데이트합니다.
- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축의 내용을 참조하십시오.

도메인 간 데이터 이동

이벤트 및 네트워크 맵은 리프 도메인과 연결되므로 리프 도메인을 상위 도메인으로 변경하는 경우 다음 두 가지 작업 중에서 선택할 수 있습니다.

- 네트워크 맵과 연결된 이벤트를 새 리프 도메인으로 이동합니다.
- 네트워크 맵을 삭제하되 이벤트는 유지합니다. 이 경우 시스템이 필요에 따라 또는 구성된 대로 이벤트를 정리할 때까지 이벤트는 상위 도메인과 연결된 상태로 유지됩니다. 또는 기존 이벤트를 수동으로 삭제할 수 있습니다.

시작하기 전에

이전의 리프 도메인이 이제 상위 도메인이 되는 도메인 컨피그레이션을 구현합니다. 도메인 관리, 5 페이지를 참조하십시오.

프로시저

단계 **1** 현재는 상위 도메인인 이전의 각 리프 도메인에 대해 다음 작업을 수행합니다.

- **Parent Domain(**상위 도메인**)**의 이벤트와 네트워크 맵을 상속할 새 **Leaf Domain(**리프 도메인**)**을 선택합니다.
- **None(**없음**)**을 선택하여 상위 도메인의 네트워크 맵을 삭제하되 기존 이벤트는 유지합니다.

단계 **2** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축의 내용을 참조하십시오.

도메인 간 디바이스 이동

글로벌 도메인 또는 두 번째 레벨 도메인에 있을 때 도메인 간에 디바이스를 이동할 수 있습니다. 도메인 간에 디바이스를 이동하면 해당 디바이스에 적용된 컨피그레이션과 정책에 영향을 줄 수 있습니다. 시스템은 자동으로 가능한 내용을 유지하고 업데이트합니다. 업데이트할 수 없는 항목, 즉 개체 재정의, 동적 라우팅 구성, 고정 경로, 진단 인터페이스와 연결된 IP 풀, DDNS를 삭제합니다.

디바이스에 원격 액세스 VPN 정책을 할당할 경우, 한 도메인에서 다른 도메인으로 동일한 디바이스를 이동할 수 없습니다.

디바이스를 이동할 때 다음과 같은 새 필수 컨피그레이션을 선택하라는 프롬프트가 표시될 수 있습니다.

- 액세스 제어 정책 - 이동한 디바이스에 할당된 액세스 제어 정책이 새 도메인에서 유효하지 않거나 액세스할 수 없는 경우 새 정책을 선택합니다. 각 디바이스에 액세스 제어 정책이 할당되어 있어야 합니다.
- 상태 정책 - 이동한 디바이스에 적용된 상태 정책이 새 도메인에서 액세스할 수 없는 경우 새 상태 정책을 선택할 수 있습니다.
- 보안 영역 - 이동한 디바이스의 인터페이스가 새 도메인에서 액세스할 수 없는 보안 영역에 속해 있는 경우 새 영역을 선택할 수 있습니다.

디바이스에서 정책을 업데이트해야 하는데 영역 간에 인터페이스를 이동할 필요가 없는 경우에는 영역 컨피그레이션이 최신 상태라는 메시지가 표시됩니다. 예를 들어 디바이스의 인터페이스가 공통 상위 도메인에 구성된 보안 영역에 속해 있는 경우에는 하위 도메인 간에 디바이스를 이동할 때 영역 컨피그레이션을 업데이트할 필요가 없습니다.

시작하기 전에

- 도메인 간에 디바이스를 이동했으며 이제 새 정책과 보안 영역을 할당해야 하는 도메인 컨피그레이션을 구현합니다. 도메인 관리, 5 페이지를 참조하십시오.

프로시저

단계 **1** **Move Devices(**디바이스 이동**)** 대화 상자의 **Select Device(s) to Configure(**구성할 디바이스 선택**)** 아래에서 구성할 디바이스를 선택합니다.

동일한 상태 및 액세스 제어 정책을 할당할 디바이스를 여러 개 선택합니다.

단계 **2** 디바이스에 적용할 **Access Control Policy(**액세스 제어 정책**)**를 선택하거나 **New Policy(**새 정책**)**를 선택하여 새 정책을 생성합니다.

단계 **3** 디바이스에 적용할 **Health Policy(**상태 정책**)**를 선택하거나 **None(**없음**)**을 선택하여 상태 정책이 없는 상태로 디바이스를 유지합니다.

단계 **4** 새 영역에 인터페이스를 할당하라는 메시지가 표시되면 나열된 각 인터페이스에 대해 **New Security Zone(**새 보안 영역**)**을 선택하거나 **None(**없음**)**을 선택하여 나중에 인터페이스를 할당합니다.

단계 **5** 영향받는 모든 디바이스를 구성한 후 **Save(**저장**)**를 클릭하여 정책 및 영역 할당을 저장합니다.

단계 **6** **Save(**저장**)**를 클릭하여 도메인 컨피그레이션을 구현합니다.

다음에 수행할 작업

- 이동의 영향을 받은 이동한 디바이스의 기타 컨피그레이션을 업데이트합니다.

- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축의 내용을 참조하십시오.

도메인 관리 기록

기능	버전	세부 사항
지원되는 최대 도메인 수 증가	6.5	이제는 도메인을 100개까지 추가할 수 있습니다. 이전에는 최대 50개의 도메인만 구축할 수 있었습니다. 지원되는 플랫폼: Firepower Management Center